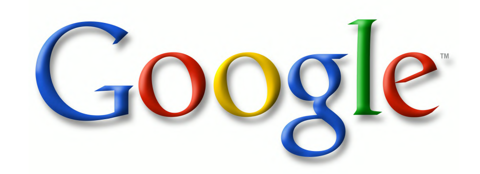



Hosted by Google

Theorie der Congruenzen

(Elemente der Zahlentheorie)

von

P. L. Tschebyscheff.

Deutsch mit Autorisation des Verfassers herausgegeben

von

Dr. Hermann Schapira,
a. o. Professor an der Universität Heidelberg.

Berlin.
Mayer & Müller.
1889.

Vorwort

des Herausgebers.

Der Name des Russischen Mathematikers P. L. Tschebyscheff ist hinreichend bekannt, um für sich selbst zu sprechen. Seine Haupt-Arbeiten, sei es in der Zahlentheorie, sei es in der Analysis oder in der Kinematik, zeichnen sich meistens ausser durch Originalität und eine gewisse Genialität hauptsächlich aus durch das Bestreben 1) *Alles durch möglich einfachste Mittel zu erreichen* und 2) *das Hauptgewicht auf die praktische Verwendbarkeit zu legen.* Diese beiden Eigenthümlichkeiten charakterisiren auch das vorliegende Lehrbuch; und es ist dasselbe darin noch nicht übertroffen worden, wiewohl es zu einer Zeit geschrieben war, wo ausser Legendre's „Théorie des nombres" und Gauss' „Disquisitiones arithmeticae" kein eigentliches Lehrbuch über diesen Gegenstand existirte. (Das Buch ist genau datirt: die erste Auflage passirte die Censur am 12/24. October 1848 und erschien 1849; die erste Auflage der vorzüglichen, von Dirichlet 1855—1858 gehaltenen Vorlesungen ist von Dedekind 1863 herausgegeben). Das strenge System in der Behandlung (zuerst die algebraischen Congruenzen und dann die Exponentielle) und die elementare Abfassung machen es möglich den ganzen Kursus, wenn man es wollte, in jeder Mittelschule durchzunehmen und eignen das Werk auch vorzüglich zum Selbstunterricht.

Die beigegebenen Tabellen, welche zum Theil auch von Jacobi für seinen „Canon arithmeticus" benutzt

worden sind*), vermehren noch die Brauchbarkeit des Buches; und ich darf hoffen mit der Deutschen Ausgabe der Litteratur nützlich gewesen zu sein, indem ich auch bemüht war eine mögliche Reinheit von Druckfehlern herzustellen. Kurze Zusätze und Bemerkungen des Herausgebers, welche hie und da, meistens behufs einer Gleichmässigkeit in dem beim Leser vorausgesetzten Kenntnissniveau nöthig schienen, sind als solche durchgehends durch eckige Klammern [ ] kenntlich gemacht

*) Vgl. Jacobi, Canon arithmeticus, introductio, pag. VII und das gegenw. Lehrb. pag. 181 und pag. 314 Anm.

Heidelberg, März 1889.

Der Herausgeber.

Vorwort

des Verfassers.

Indem ich bei der Abfassung einer *„Theorie der Congruenzen“* den Werken *„Théorie des nombres“* von Legendre und *„Disquisitiones arithmeticae“* von Gauss nicht ganz gefolgt bin, erachte ich es für nothwendig, die Ursachen anzugeben, welche mich veranlassten, von diesen vorzüglichen Werken der beiden berühmten Mathematiker abzuweichen. Zu dem Ende werde ich in einige Einzelheiten bezüglich der genannten Werke und des dermaligen wissenschaftlichen Zustandes der Zahlentheorie einzugehen haben.

Die Grundlage zu allen Untersuchungen, welche den allgemeinen Theil der Zahlentheorie ausmachen, ist von Euler geschaffen. Den Forschungen Euler's waren vorangegangen die von Fermat, der sich zuerst mit den Eigenthümlichkeiten von Zahlen, die gewissen unbestimmten Gleichungen zu genügen haben, beschäftigt hat. Die Untersuchungen Fermat's ergaben als Resultat die Entdeckung vieler allgemeiner Theoreme der Zahlentheorie; indess übten sie ihren Einfluss nicht unmittelbar auf die Entwickelung der Wissenschaft, indem die Sätze von Fermat ohne Beweis und ohne Anwendung blieben. In diesem Zustande dienten die Entdeckungen Fermat's den Mathematikern nur als Herausforderung zum tiefern Eindringen in die Theorie der Zahlen. Aber wie interessant auch diese Untersuchungen waren, bis Euler hatte sich Niemand dazu gemeldet. Das ist auch begreiflich.

Nicht um neue Anwendungen bereits bekannter Methoden, auch nicht um weitere Entwickelungen früher bereits verwendeter Methoden handelte es sich bei diesen Untersuchungen; vielmehr mussten für dieselben neue Methoden geschaffen, neue Principien entdeckt werden, mit einem Worte: eine neue Wissenschaft musste begründet werden. Dieses ist durch Euler geschehen.

Unter den vielen Untersuchungen Euler's auf dem Gebiete der Zahlentheorie haben den meisten Einfluss auf den Erfolg dieser Wissenschaft seine Abhandlungen über folgende zwei Gegenstände gehabt:

1) Ueber die Potenzen der Zahlen bezüglich der Reste, welche sie bei ihrer Division durch eine gegebene Zahl ergeben.
2) Ueber Zahlen, welche als Summe zweier Zahlen dargestellt werden, von denen eine ein Quadrat und die andere ein Product aus einem Quadrate und einer gegebenen Zahl bildet.

Die Abhandlungen über den ersten Gegenstand gaben die Grundlage zur Theorie der Indices, zur Theorie der binomischen Congruenzen überhaupt und derjenigen der quadratischen Reste insbesondere; die Abhandlungen über den zweiten Gegenstand bildeten den Anfang einer Theorie quadratischer Formen.

Die Grundlage zur Theorie der Indices schuf Euler mit seinem Memoire:

„Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia“, welches in den Memoiren der St. Petersburger Academie der Wissenschaften für das Jahr 1773 erschienen ist. In diesem Memoire entdeckt Euler die Eigenschaften der Indices und der primitiven Wurzeln, zeigt ferner eine obere Grenze für die Anzahl der möglichen Lösungen binomischer Congruenzen mit Primzahlmodul und giebt endlich eine Anwendung der Theorie der Indices auf die Theorie der quadratischen Reste und die der quadratischen Formen. Zur Vervollkommnung der Theorie der Indices blieb noch die Auffindung einer Methode zur Bestimmung der primitiven Wurzeln, ohne Versuche an verschiedenen Zahlen anstel-

len zu müssen. Alle Anstrengungen Euler's in dieser Beziehung waren vergeblich; er sagt:

„*Via quidem adhuc non patet, tales radices primitivas pro quovis divisore primo inveniendi, neque etiam demonstratio, qua tales radices primitivas semper dari e vici, methodum eas inveniendi declarat*“ *).

Aber noch heute sind wir, ungeachtet aller Erfolge der Zahlentheorie, bei der Auffindung primitiver Wurzeln, noch immer darauf angewiesen, es mit verschiedenen Zahlen zu probieren und die von mir im zweiten Anhange gegebenen Lehrsätze dürften wohl etwa den ersten Versuch bilden zur Auffindung primitiver Wurzeln ohne vorhergehendes Probieren.

Die Untersuchungen Euler's über die Theiler der Zahlen von der Form $a^n \pm b^n$ bildeten den Anfang zu einer Theorie binomischer Congruenzen. Wir finden diese Untersuchungen in vielen Memoiren Euler's; besondere Beachtung verdient darunter sein Memoir „*Theoremata circa divisores numerorum*“. Darin wird gezeigt, dass die Möglichkeit, die Congruenz

$$x^n - a \equiv 0 \pmod{mn+1}$$

zu befriedigen, wenn $mn+1$ eine Primzahl ist, die Theilbarkeit von

$$a^m - 1$$

durch diese Primzahl voraussetzt und auch die Umkehrung des Satzes wird daselbst unter der Annahme bewiesen, dass m und n relativ prim zu einander seien. Abgesehen von der unnöthigen Beschränkung auf m und n, welche relativ prim sind, bilden diese Sätze die Grundlage der heutigen Theorie der binomischen Congruenzen überhaupt und der Theorie der quadratischen Reste insbesondere. Betrachtet man den Beweis des letztgenannten Satzes bei Euler näher, so ist es übrigens leicht die Erweiterung des Satzes auf beliebige m und n zu bemerken. In seinem Memoire: „*De quibusdam eximiis proprietatibus circa divisores potestatum occurentibus*“ beweist

*) Op. min. col. t. 1, pag. 523.

er es insbesondere für $m = 2$, ohne irgend welche Beschränkungen für n zu machen und zeigt, dass die Theilbarkeit von $a^n - 1$ durch $2n + 1$ die nothwendige und hinreichende Bedingung ist, damit a quadratischer Rest der Zahl $2n + 1$ sei. Ausserdem beschäftigte sich Euler in anderen Memoiren vielfach mit den quadratischen Resten und in den *„Observationes circa divisionem quadratorum per numeros primos“* gelangt er bei der Betrachtung der Reste, welche bei der Division von Quadraten durch Primzahlen erhalten werden, zu folgendem Schlusse:

> Existente s numero quocunque primo, dividantur tantum quadrata imparia
>
> $$1, \quad 9, \quad 25, \quad 49, \quad \ldots .$$
>
> per divisorem $4s$, notenturque residua, quae omnia erunt formae $4q + 1$, quorum quodvis littera α indicetur, reliquorum autem numerorum, formae $4q + 1$, qui inter residua non occurrunt, quilibet littera $\mathfrak{a}$ indicetur, quo facto si fuerit

divisor numerus primus formae	tum est
$4ns + \alpha$	$+s$ residuum et $-s$ residuum
$4ns - \alpha$	$+s$ residuum et $-s$ non-residuum
$4ns + \mathfrak{a}$	$+s$ non-residuum et $-s$ non-residuum
$4ns - \mathfrak{a}$	$+s$ non-residuum et $-s$ residuum.

Diese Entdeckung finden wir bei Euler im 1ten Bande der Opuscula analytica, 1772. Es ist nicht schwer darin das *Reciprocitätsgesetz zweier Primzahlen* zu erkennen, welches von Legendre im Jahre 1785 publicirt und welches Letzterer zur Grundlage der Theorie der quadratischen Reste gemacht hat.

In der Theorie der quadratischen Formen beginnt Euler seine Untersuchungen mit der Summe zweier Quadrate und zeigt im Memoire *„De numeris, qui sint aggregata duorum quadratorum“*, dass die Theiler einer Summe zweier Quadrate, welche zu einander relativ prim sind, eine ähnliche Summe bilden müssen und erhält eine lineare Form für diese Theiler. Und so kommt er auf das berühmte Theorem von Fermat über die Zerlegung einer

Primzahl von der Form $4m + 1$ in eine Summe von zwei Quadraten. In analoger Weise findet Euler die quadratischen und linearen Theiler einer Summe eines Quadrates und des zweifachen oder dreifachen anderen Quadrates und giebt ferner ohne Beweis die linearen Formen der Theiler vieler anderer quadratischer Formen. So hat Euler die Grundlage geschaffen zu einer Theorie der Theiler quadratischer Formen. Die genialen Entdeckungen, welche Lagrange in diesem Theile der Zahlentheorie macht, eröffnen wieder Euler den Weg zu neuen Forschungen. Als Ergebniss derselben entstand eine neue Entwickelung der Theorie der quadratischen Formen mit mehreren Anwendungen derselben auf die Untersuchung, ob eine gegebene Zahl Primzahl ist oder nicht und auf die Auffindung von ausserordentlich grossen Primzahlen.

Euler hat sich in seinen Untersuchungen nicht auf *endliche* Formeln allein beschränkt; er zeigte auch wie man mit Hülfe von unendlichen Reihen auf verschiedene Theoreme der Zahlentheorie kommen kann. Zu diesen Untersuchungen gehören diejenigen „*De partitione numerorum*“ und die „*über die Summen der Theiler verschiedener Zahlen*“.

Da wir die Entwickelung des allgemeinen Theiles der Zahlentheorie im Auge haben, so wollen wir uns bei den Untersuchungen Euler's über *Diophant*ische Analysis nicht aufhalten, welche zum Resultate hatten die Lösung von Gleichungen von der Form $ax^2 + by^2 = cz^2$, ferner den Beweis der Unmöglichkeit gewisser Gleichungen mit zwei und drei Unbekannten, wie auch die Lösung vieler sehr complicirter unbestimmter Gleichungen und wenden uns zu den Untersuchungen von

Lagrange, durch welche die allgemeinen Grundlagen der Zahlentheorie sehr wichtige Erweiterungen erfahren haben. Dahin gehören seine Untersuchungen über die Anzahl der Lösungen, welche Congruenzen mit Primzahlmodul zulassen, und die Untersuchungen über die Eigenschaften quadratischer Formen. Wir haben gesehen, dass von Euler eine obere Grenze gefunden war für die Anzahl der Lösungen binomischer Congruenzen; Lagrange

hat bewiesen, dass dieselbe obere Grenze auch für ein beliebiges Polynom bestehen bleibt. Mit dieser Entdeckung ermöglichte es Lagrange viele Sätze der Zahlentheorie zu beweisen, deren Beweis sonst unüberwindliche Schwierigkeiten bereiteten. Zu diesen Sätzen müssen diejenigen über die Existenz primitiver Wurzeln für alle Primzahlen gezählt werden. Der von Euler vorgeschlagene Beweis stützt sich auf die Eigenschaft binomischer Congruenzen, welche nur nach der Entdeckung Lagrange's streng bewiesen werden kann. Aber unter allen Arbeiten Lagrange's in der Zahlentheorie haben den grössten Einfluss auf die Erfolge dieser Wissenschaft seine Untersuchungen über quadratische Formen gehabt. Er gab allgemeine Principien für diejenigen Untersuchungen, welche Euler nur für einige der einfachsten Formen gefunden hatte; und diese Principien bildeten, nachdem sie von Legendre weiter entwickelt wurden, eine vollständige Theorie der Theiler quadratischer Formen; diese Theorie ist eine der bedeutendsten in der Zahlentheorie überhaupt und besonders wichtig durch ihre Anwendungen auf die Bestimmung der Theiler einer gegebenen Zahl.

Die von Legendre gelieferten Entwickelungen der quadratischen Formen waren eine Folge seiner Entdeckungen in der Theorie der quadratischen Reste. Die Schlussfolgerung, welche wir oben aus der Abhandlung Euler's *Observationes circa divisionem quadratorum per numeros primos* angeführt haben, enthält den Satz, welchen wir heute unter dem Namen *„Reciprocitätsgesetz zweier Primzahlen“* kennen, und welchem die Theorie der quadratischen Reste ihre Erfolge verdankt. In den Memoiren der Pariser Academie der Wissenschaften für das Jahr 1785 beweist Legendre den genannten Satz vermittelst der von ihm entdeckten Kriterien für die Möglichkeit der Gleichung $ax^2 + by^2 = cz^2$ und giebt auch Anwendungen des Satzes auf die Untersuchung der Congruenzen zweiten Grades und auf die Bestimmung der Theiler quadratischer Formen.

In diesem Zustande befanden sich die verschiedenen Theile der Zahlentheorie, als Legendre sein Werk schrieb *„Essai sur la Théorie des nombres“*, welches er

später mit vielen Zusätzen, aber ohne wesentliche Veränderung in dem Systeme der Behandlung der Hauptheile, unter dem Namen „*Théorie des nombres*“ herausgegeben hat.

Bei aller hohen Entwickelung einzelner Theile der Zahlentheorie stiess doch eine systematische Zusammenstellung dieser Wissenschaft auf unüberwindliche Schwierigkeiten. Wir haben gesehen, dass das *Reciprocitätsgesetz zweier Primzahlen*, welches die Grundlage der Theorie der quadratischen Reste ausmacht und mithin für die Theorie der quadratischen Formen unumgänglich ist, von Legendre aus den Eigenschaften einer Gleichung zweiten Grades hergeleitet worden ist. Daher konnte die Theorie der quadratischen Reste und Formen erst nach der vorangegangenen Theorie der unbestimmten Gleichungen zweiten Grades behandelt werden. Diese Theorie liegt aber ihrem Wesen nach viel höher und lässt ihrerseits eine Anwendung der Theorie der quadratischen Reste zu. Infolgedessen fängt Legendre, nachdem er in seinem Werke verschiedene Sätze über Zahlen vorausgeschickt hat, mit der Lösung unbestimmter Gleichungen an und erst, nachdem er eine vollständige Theorie der Gleichungen zweiten Grades auseinandergesetzt hat, schreitet er zu den *allgemeinen Eigenschaften der Zahlen*, unter denen wir bei ihm die Hauptsätze der Theorie der Congruenzen und eine vollständige Theorie der quadratischen Reste und der quadratischen Formen finden. Diese, eines Systems ermangelnde Anordnung in der Abfassung der Hauptheile der allgemeinen Zahlentheorie, blieb nur so lange nothwendig bis Gauss zeigte, wie man das *Reciprocitätsgesetz zweier Primzahlen* direct aus der Betrachtung von Congruenzen herleiten kann. Auf diese Weise eröffnete sich die Möglichkeit, die Congruenzen zweiten Grades, ohne in den Hauptheilen der Zahlentheorie die systematische Anordnung zu zerstören, zusammen mit den anderen Congruenzen zu behandeln, bevor man zu den Gleichungen zweiten Grades gekommen ist; und nachher, vermittelst der Resultate der Theorie der Congruenzen die Untersuchung von Gleichungen höheren Grades zu vereinfachen.

Wir wenden uns nunmehr zu dem Werke von Gauss. Wir haben gesehen welche Entwickelungen in den verschiedenen Theilen der Zahlentheorie durch die Arbeiten von Euler, Lagrange und Legendre gemacht waren. Gauss benutzt indess in seinem Werke *Disquisitiones arithmeticae* die Untersuchungen jener Mathematiker nicht. Unabhängig von denselben entwickelt er die Haupttheile der Zahlentheorie, indem er sie durch neue Methoden, durch neue Entdeckungen und sehr wichtige Anwendungen auf die Lösung binomischer Gleichungen bereichert. Aber bei allen Verdiensten des Gauss'schen Werkes können wir nicht umhin zu erkennen, dass ein grosser Theil seiner Herleitungen nicht die Einfachheit besitzt, durch welche das Verfahren von Euler, Lagrange und Legendre sich auszeichnet. In dieser Beziehung kann man seiner Entwickelung einzelner Theile der Zahlentheorie, mit Ausnahme einiger, nicht vor den Auseinandersetzungen Legendre's den Vorzug geben.

Daraus ist ersichtlich, dass weder das Werk von Legendre, noch das von Gauss die Zahlentheorie in derjenigen vollkommnen Form darstellt, in welcher sie nach den Entwickelungen, welche dieselbe durch die Arbeiten dieser Mathematiker, geschweige erst nach den Arbeiten der jüngsten Mathematiker dargestellt werden kann. Ich konnte mich daher bei der Zusammenstellung der Theorie der Congruenzen weder an Legendre allein, noch an Gauss allein halten, vielmehr benutzte ich zugleich mit Legendre und Gauss, auch noch die Arbeiten vieler anderer Mathematiker, welche sich mit diesem Theile der Zahlentheorie beschäftigt haben. Um aber die Untersuchungen der Mathematiker, welche sehr verschiedenartige Methoden benutzten, in ein System zu bringen, musste ich einen grossen Theil ihrer Schlussfolgerungen ändern. Ausserdem fand ich es der Vollständigkeit willen für nothwendig, einige Artikel weiter auszubilden. So betrachte ich in der Theorie der Congruenz ersten Grades drei verschiedene Fälle, wann diese Congruenz *eine* Lösung hat, wann sie deren *mehrere* und wann sie *gar keine* besitzt. Bei der Auseinandersetzung der

Eigenschaften der Congruenzen höheren Grades gebe ich ausser dem Lagrange'schen Satze, einige diesbezügliche allgemeine Sätze. In der Theorie der quadratischen Formen gebe ich eine Methode, vermittelst deren man erkennen kann, wann zwei quadratische Formen der Theiler lediglich auf lineare Formen zurückführbar sind. Ausserdem finden sich in meinem Buche drei Anhänge. In dem ersten setze ich die Jacobi'sche Erweiterung des Legendre'schen Zeichens auseinander und gebe eine Anwendung desselben auf die Untersuchung der quadratischen Reste; in der zweiten beweise ich einige Theoreme, welche die primitiven Wurzeln einiger Zahlen direct aus ihrer Gestalt bestimmen lassen; in der dritten gebe ich die Resultate meiner Untersuchungen über die Eigenschaften von Functionen, welche bestimmen wie viele Primzahlen eine gegebene Zahl nicht übertreffen.

[Der dritte Anhang über die Anzahl der Primzahlen ist, weil er seinem Wesen nach nicht so elementar ist als der Inhalt dieses Lehrbuches, auf Wunsch des Verfassers hier fortgelassen worden].

Inhaltsverzeichniss.

Einleitende Vorbegriffe.

Kapitel I.

Ueber Congruenzen im Allgemeinen.

Kapitel II.

Ueber die Congruenzen ersten Grades.

Kapitel VI.

Ueber Congruenzen von der Gestalt $a^x \equiv A$ (mod. p).

Kapitel VII.

Ueber Congruenzen zweiten Grades mit zwei Unbekannten.

Kapitel VIII.

Anwendung der Theorie der Congruenzen auf die Zerlegung von Zahlen in Primzahlfactoren.

Anhang I.



Tabellen:

[*) In den russischen Ausgaben reichte diese Tabelle nur bis zur Primzahl 5987].

Bemerkte Druckfehler.

Seite 11	Zeile	4	v. u.	Die Gleichung soll mit (2) numerirt werden.
» 175	»	13	» »	Lies: beweisen wir in.
» 186	»	16	v. o.	Statt (mod. p), lies: (mod. $p-1$).
» »	»	19	» »	Statt wenn q, lies: wenn Ind. q.
» 202	»	6	» »	Ergänze die fehlende Congruenz $x \equiv 3^5$;
» „	»	9	» »	Ergänze die zwischen 3 und 10 fehlende Zahl 5.

Tabellen.

pag. 8 Primzahl 59 Tilge die primitive Wurzel 57, und setze dafür 56.



Theorie der Congruenzen.

Einleitende Vorbegriffe.

§ 1. Ueber das Wesen der Zahlentheorie und der Theorie der Congruenzen.

Die Zahlentheorie, oder anders genannt, die Transcendente Arithmetik ist die Wissenschaft, welche von der Lösung unbestimmter Gleichungen in ganzen Zahlen handelt.

Während diese Wissenschaft den Begriff der *Zahlen* der Arithmetik und den der *Gleichungen* der Algebra und der transcendenten Analysis entleiht, ist sie gleichwohl von beiden letzteren Wissenschaften wesentlich verschieden. Von der Arithmetik unterscheidet sich die Zahlentheorie insofern, als sie die Zahlen lediglich in Bezug auf ihre Fähigkeit unbestimmten Gleichungen dieser oder jener Art zu genügen untersucht und somit vollkommen unabhängig bleibt von dem Numerationssysteme, auf welchem die arithmetischen Operationen gegründet sind. Von der Algebra und den anderen Theilen der bestimmten Analysis unterscheidet sie sich dadurch, dass sie sich bei der Untersuchung der Gleichungen auf die ganzzahligen Werthe der Unbekannten beschränkt.

Durch ihre eigenthümliche Betrachtung der Zahlen sowohl, als der Gleichungen von einem ganz besonderen Gesichtspunkte aus, gelangt die Zahlentheorie auf diese Weise zu vollkommen neuen Resultaten, welche dann zugleich für die Arithmetik und für die Theorie der be-

stimmten Gleichungen von höchster Bedeutung werden. Der Arithmetik erleichtert sie Rechnungen, welche sonst wegen ungeheurer Weitläufigkeit, unausführbar gewesen wären. Der Algebra öffnet sie einen Weg zur Lösung von Aufgaben, welche ohne ihre Hülfe als unlösbar erscheinen.

Jede Gleichung, welche mehrere Veränderliche, oder Unbekannte enthält, unterliegt einer Untersuchung von Seiten der Zahlentheorie.

Indess sind nicht alle Gleichungen für die Untersuchung gleich zugänglich, auch nicht alle von gleich hoher Wichtigkeit in Bezug auf ihre Anwendbarkeit.

In ihrem gegenwärtigen Zustande beschränkt sich die Zahlentheorie auf die Betrachtung der *allereinfachsten* Gleichungen, welche zugleich die *wichtigsten* Anwendungen zulassen.

Unter diesen Gleichungen verdienen diejenigen eine besondere Aufmerksamkeit, welche eine der Unbekannten nur in der ersten Potenz enthalten; sie sind bemerkenswerth sowohl durch ihre besonderen Eigenschaften, als auch durch ihre Anwendbarkeit auf die Vereinfachung arithmetischer Operationen und auf die Lösung von Aufgaben, welche die bestimmte Analysis betreffen.

Solche Gleichungen sind es nun, welche den Gegenstand der Untersuchung für die Theorie der Congruenzen ausmachen.

---

§ 2. Ueber absolute Primzahlen.

Bevor wir die Untersuchung der zuletzt hervorgehobenen Gleichungen aufnehmen, werden wir uns ein wenig bei denjenigen Eigenschaften der Zahlen, welche zum Theil aus der Arithmetik bekannt sind, aufhalten, um dieselben, entsprechend ihrer Wichtigkeit, hier eingehend auseinander zu setzen.

Man theilt die Zahlen ein in einfache und zusammengesetzte Zahlen.

Einfach heisst eine Zahl, welche nur durch *Eins* und

durch sich selbst theilbar ist; eine solche wird auch *Primzahl* genannt. *Eine zusammengesetzte Zahl* nennt man dagegen eine solche, welche durch eine andere Zahl, die grösser als *Eins* ist, ohne Rest getheilt werden kann. So sind

2, 3, 5, 7, 11, und viele andere

Primzahlen, hingegen

4, 6, 8, 9, 10 und andere dergleichen

zusammengesetzte Zahlen.

Man kann sich leicht überzeugen, dass es eine *unendliche Menge von Primzahlen* giebt.

Denn, lassen wir das Gegentheil zu und nehmen an, es gebe eine gewisse endliche Zahl, welche die allergrösste unter allen überhaupt vorkommenden Primzahlen wäre und bezeichnen dieselbe mit N, so müssen wir zugeben, dass alle Zahlen, welche grösser als N sind, lauter zusammengesetzte Zahlen seien, welche also durch Multiplication von gewissen Potenzen der Zahlen

$$2,\ 3,\ 5,\ 7,\ 11,\ \ldots,\ N$$

entstehen.

Die Unrichtigkeit dieser Annahme geht aber aus der Zahl M, welche durch die Gleichung

$$M = 1.2.3.4.5.\ldots.(N-1)\,N+1$$

definirt ist, klar hervor, indem M offenbar grösser als N ist und doch durch keine der Zahlen

$$2,\ 3,\ 5,\ 7,\ 11,\ \ldots,\ N$$

ohne Rest theilbar ist und somit nicht aus der Multiplication von Potenzen dieser letzteren Zahlen entstehen kann. Folglich ist die Annahme,

es gebe nicht unendlich viele Primzahlen,

unzulässig.

Das allereinfachste Mittel, um alle Primzahlen, welche kleiner als eine gegebene Grenzzahl N sind, zu erhalten, besteht darin, dass man in der Reihe der Zahlen

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12,\ 13,\ 14,\ \ldots,\ N-1,\ N$$

nach und nach alle Vielfachen von

$$2, 3, 5, 7, 11, \ldots . \text{ etc.}$$

fortlässt. Dieses erreicht man offenbar dadurch, dass man in der Zahlenreihe

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, \ldots, N-1, N$$

jede zweite Zahl, anfangend hinter der 2, durchstreicht, dann ebenso jede dritte Zahl hinter der 3, darauf jede vierte Zahl hinter der 4 etc. und ebenso allgemein jede $n$te Zahl, anfangend hinter der Zahl n. Auf diese Weise werden alle zusammengesetzten Zahlen [mitunter auch mehrfach*)] durchstrichen, und undurchstrichen bleiben nur die Primzahlen allein übrig.

---

§ 3. **Ueber relative Primzahlen.**

Zwei oder mehrere Zahlen heissen relativ prim zu einander, wenn sie keinen gemeinschaftlichen Factor (Theiler) besitzen. So sind die Zahlen 10 und 21 relativ prim zu einander. Aus dieser Definition *relativer Primzahlen* folgt, als specieller Fall, dass

wenn A selbst eine Primzahl ist und B nicht theil-

[*) Dieses Verfahren ist, weil dasselbe gewissermassen ein Aussieben der Nicht-primzahlen bedeutet, unter dem Namen *cribrum* Eratosthenis, nach seinem Erfinder Eratosthenes (276 oder 275 v. Chr. geb. und ungef. 194 gest.) bekannt. Bei Eratosthenes sollen überhaupt nur die ungeraden Zahlen allein von vornherein aufgeschrieben werden, weil die 2, indem sie gerad ist, nach Jamblichus keine Primzahl sei, trotzdem sie Euclid „fehlerhafter Weise" unter die Primzahlen gezählt habe. Vgl. Cantor, Geschichte der Mathematik, pag. 286. Die Regel für das Durchstreichen würde dann allgemein lauten müssen: man durchstreiche jede $(2n+1)^{\text{te}}$ Zahl hinter $(2n+1)$. Die Bemerkung, dass man keine durchstrichene Zahl als Ausgangspunkt einer neuen Aussiebung benutzen soll, ist (obwohl auch bei Legendre aufgenommen) *nicht nothwendig* und wohl deshalb hier weggelassen. Allerdings *reicht es hin*, wenn man die einmal durchstrichenen Zahlen nicht wieder benützte; indess erhält man, wenn man sie wieder benutzt, das Gesetz: jede Zahl $N = \alpha^m \beta^n \gamma^p \ldots$ wird genau $[(m+1)(n+1)(p+1)\ldots -2]$ mal durchstrichen.]

bar durch A, so sind A und B relativ prim zu einander.

Es können nämlich in der That A und B in diesem Falle weder einen (von A verschiedenen) gemeinschaftlichen Theiler besitzen, weil A als Primzahl durch keine andere Zahl theilbar sein kann; noch können sie A selbst als gemeinschaftlichen Theiler besitzen, da nach der Voraussetzung B durch A nicht theilbar ist.

Bemerken wir, dass, wenn B kleiner als A ist, dann B überhaupt durch A nicht theilbar sein kann, so können wir dem Obigen gemäss schliessen, dass wenn B kleiner als A ist und A selbst eine Primzahl, so müssen die Zahlen A und B relativ prim zu einander sein. Diese Eigenschaft der Zahlen können wir so aussprechen:

Jede Zahl, welche kleiner ist als eine gegebene Primzahl, ist zu derselben relativ prim.

So sind die Zahlen

$$2, 3, 4, 5, 6, 7, 8, 9, 10,$$

relativ prim zu 11.

Daraus folgt ferner:

Beliebige (von einander verschiedene) Primzahlen sind relativ prim zu einander.

---

§ 4. **Eigenschaften relativer Primzahlen.**

Wir wollen nunmehr uns eingehender mit den Eigenschaften solcher Zahlen beschäftigen, welche relativ prim zu einander sind.

1. *Lehrsatz. Sind die Zahlen A und B einzeln relativ prim zu einer Zahl S, so ist auch ihr Product AB relativ prim zu S.*

Beweis. Um diesen Lehrsatz zu beweisen, suchen wir zunächst den grössten gemeinschaftlichen Theiler von A und S. Zu diesem Ende muss man, wie aus der Arithmetik bekannt ist, vorerst A durch S dividiren; durch den gefundenen Rest dividirt man dann S; durch den neuerdings gefundenen Rest dividirt man darauf den ersten

Rest u. s. w. Der letzte Rest wird in unserem Falle 1 sein; weil A und S, als relative Primzahlen, keinen von 1 verschiedenen gemeinschaftlichen Theiler besitzen können. Bezeichnen wir die durch die ebengedachten Divisionen successive erhaltenen Quotienten mit

$$q, q_1, q_2, \ldots, q_{n-2}, q_{n-1}, q_n$$

und die entsprechenden zugehörigen Reste mit

$$r, r_1, r_2, \ldots, r_{n-2}, r_{n-1}, r_n,$$

setzen den jedesmaligen Dividendus gleich dem Producte aus Divisor und Quotienten plus dem zugehörigen Reste und berücksichtigen, dass der letzte Rest r_n in unserem Falle 1 ist, so erhalten wir folgende Gleichungen:

$$\begin{aligned} A &= Sq + r, \\ S &= rq_1 + r_1, \\ r &= r_1 q_2 + r_2, \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + 1, \end{aligned}$$

welche durch Multiplication mit B in

$$(1) \quad \ldots \quad \left\{ \begin{aligned} AB &= BSq + Br, \\ BS &= Brq_1 + Br_1, \\ Br &= Br_1 q_2 + Br_2, \\ &\vdots \\ Br_{n-2} &= Br_{n-1} q_n + B \end{aligned} \right.$$

übergehen. Die erste dieser Gleichungen sagt aus, dass ein gemeinschaftlicher Theiler von AB und S auch ein Theiler von Br sein muss; die zweite —, dass derselbe Theiler zugleich auch ein Theiler von Br_1; die dritte —, dass er auch ein Theiler von Br_2; etc. und die letzte Gleichung sagt dann, dass ein gemeinschaftlicher Theiler von AB und S auch B ohne Rest theilen wird.

Da aber B und S nach Voraussetzung keinen gemeinsamen Theiler besitzen, so können auch AB und S keinen solchen haben, was zu beweisen war.

Indem wir diesen Lehrsatz auf mehrere Zahlen A, B, C, D, ... ausdehnen, welche zu S_0, S_1, S_2, ... relativ prim sind, überzeugen wir uns leicht von der Richtigkeit des allgemeineren Satzes:

Die Producte $A\,B\,C\,D\,\ldots\ldots$ und $S_0\,S_1\,S_2\,\ldots\ldots$ sind relativ prim zu einander, falls die Zahlen $A, B, C, D, \ldots\ldots$ einzeln relativ prim sind zu einer jeden der Zahlen $S_0, S_1, S_2, \ldots\ldots$

Ferner können wir folgende Lehrsätze leicht beweisen:

2. *Lehrsatz. Ist eine Zahl S ein Divisor eines Productes AB und relativ prim zu einem der Factoren A, so ist dieselbe ein Divisor des anderen Factors B.*

Beweis. Wir stellen wiederum die Gleichungen (1) her und bemerken, dass die Theilbarkeit von AB durch S die Theilbarkeit der Zahlen

$$Br,\ Br_1,\ Br_2,\ \ldots\ldots$$

und schliesslich auch B durch S voraussetzt; w. z. b. w.

3. *Lehrsatz. Ist von zwei Zahlen A und B, welche zu einander relativ prim sind, eine jede ein Theiler von S, so ist auch das Product derselben AB ein Theiler von S.*

Beweis. Bezeichnen wir den Quotienten, welcher aus der Division von S durch A erhalten wird, mit L, so haben wir für S die Bestimmung

$$S = AL,$$

woraus die Theilbarkeit von AL durch B folgt, weil nach der Voraussetzung S durch B theilbar ist. Nach dem vorhergehenden Lehrsatze setzt aber die Theilbarkeit von AL durch B, wenn B relativ prim zu A ist, voraus, dass L durch B theilbar sein muss. Bezeichnen wir also den Quotienten, welcher bei dieser Division von L durch B entsteht, mit M, so erhalten wir die Gleichung

$$L = BM,$$

der zufolge die obige Gleichung in

$$S = ABM$$

übergeht. Daraus wird aber die Theilbarkeit von S durch AB, welches wir ja beweisen wollen, augenscheinlich.

Dehnen wir diesen Lehrsatz auf mehrere Zahlen aus, so können wir allgemein schliessen, dass

> *wenn eine Zahl S durch jede der Zahlen A, B, C, D, ... theilbar ist und A, B, C, D, ... relativ prim zu einander sind, dieselbe Zahl S durch das Product $ABCD$ . . . . theilbar sein muss.*

---

§ 5. Ueber die Zerlegung der Zahlen in Primzahlfactoren.

Wir wollen nunmehr zu denjenigen Eigenschaften der Zahlen übergehen, welche bei ihrer Zerlegung in Primzahlfactoren zum Vorschein kommen.

Aus der Arithmetik ist bekannt, dass jede Zahl als Product von lauter Primzahlen dargestellt werden kann [*)]. Indem wir nun die verschiedenen Primzahlen, welche in einer Zahl N als Factoren enthalten sind, mit $\alpha, \beta, \gamma, \ldots.$ und die entsprechenden Potenzen, in welchen jede dieser Primzahlen in N vorkommt, beziehungsweise mit $m, n, p, \ldots.$ bezeichnen, erhalten wir

$$N = \alpha^m \beta^n \gamma^p \ldots.$$

Aus dieser Gleichung schliessen wir auf Grund des Lehrsatzes 1, *dass N relativ prim ist zu allen Primzahlen, welche von $\alpha, \beta, \gamma, \ldots.$ verschieden sind.*

In der That ist jede von $\alpha, \beta, \gamma, \ldots.$ verschiedene Primzahl, nach § 3, relativ prim zu jeder dieser Primzah-

---

[*) Dieser Satz, dass jede Zahl als Product von lauter Primzahlfactoren zu betrachten ist, darf hier direct der Arithmetik entnommen werden, weil letztere den Beweis dafür offenbar aus den obigen Definitionen folgern kann.

Ist nämlich eine Zahl N nicht selbst Primzahl, so enthält dieselbe, nach der Definition in § 2, von Eins und von N verschiedene Factoren, welche, falls sie nicht Primzahlen sind, ihrerseits wiederum neue Factoren enthalten etc. Da aber die Fortsetzung dieser Schlussweise auf immer kleiner werdende Zahlen führt, so muss man endlich auf lauter Primzahlfactoren kommen, welche allerdings zum Theil einander gleich sein dürfen; oder, mit anderen Worten:

> In jeder endlichen Zahl N ist immer und nur eine endliche Anzahl Potenzen von Primzahlen als Factoren enthalten.]

len $\alpha, \beta, \gamma, \ldots.$ und folglich auch zu ihrem Producte $\alpha \beta \gamma \ldots.$ und mithin, nach Lehrsatz 1, auch relativ prim zu $\alpha^m \beta^n \gamma^p \ldots.$ Daraus können wir nun allgemein schliessen, dass keine Zahl durch eine Primzahl theilbar sein kann, welche nicht in derselben als Factor enthalten ist. Es kann also die Zahl N, von welcher wir

$$N = \alpha^m \beta^n \gamma^p \ldots.$$

vorausgesetzt haben, nur theilbar sein durch gewisse Potenzen der Primzahlen $\alpha, \beta, \gamma, \ldots.$, welche in derselben enthalten sind. Was nun die Potenzen betrifft, so kann man sich leicht überzeugen, dass eine Theilbarkeit durch $\alpha^{m'}$, wenn $m' > m$, ebenso durch $\beta^{n'}$, wenn $n' > n$, oder durch $\gamma^{p'}$, wenn $p' > p$ etc. nicht möglich ist. Denn da $N = \alpha^m \beta^n \gamma^p \ldots.$ ist, so wird der Quotient aus der Division von N durch $\alpha^{m'}$ in der Gestalt eines Bruches

$$\frac{\alpha^m \beta^n \gamma^p \ldots.}{\alpha^{m'}}, \text{ oder } \frac{\beta^n \gamma^p \ldots.}{\alpha^{m'-m}}$$

erhalten werden, welcher für $m' > m$ keinesfalls eine ganze Zahl werden kann, weil α als eine von $\beta, \gamma, \ldots.$ verschiedene Primzahl, nach unserer soeben gemachten Bemerkung das Product $\beta^n \gamma^p \ldots.$ nicht ohne Rest theilen kann. Mithin kann N nur theilbar sein durch solche Potenzen von $\alpha, \beta, \gamma, \ldots.$, welche respective die $m$te, $n$te, $p$te, ... Potenz nicht überschreiten. Folglich ist N nur durch solche Zahlen theilbar, in welchen die Primzahlen $\alpha, \beta, \gamma, \ldots.$ zu Potenzen enthalten sind, die resp. die $m$te, $n$te, $p$te, ... Potenz nicht übertreffen. Somit erhalten wir folgenden

4. *Lehrsatz.* *Eine Zahl N ist durch eine Zahl M nur dann theilbar, wenn alle Primzahl-Factoren von M in N enthalten sind und ihre Potenzen in N nicht niedriger sind als in M.*

Auf Grund dieses Lehrsatzes beweisen wir nun folgenden

5. *Lehrsatz.* *Für eine Zahl N ist nur eine einzige Zerlegung in Primzahl-Factoren möglich.*

Beweis. Nehmen wir an, es gäbe für eine Zahl N zweierlei Zerlegungen in Primzahl-Factoren, wie etwa:

$$N = \alpha^m \beta^n \gamma^p \ldots.; \quad N = \alpha_1^{m'} \beta_1^{n'} \gamma_1^{p'} \ldots.,$$

so würden wir durch Division je einer dieser Gleichungen durch die andere die Relationen erhalten:

$$\frac{\alpha^m \beta^n \gamma^p \ldots.}{\alpha_1^{m'} \beta_1^{n'} \gamma_1^{p'} \ldots.} = 1; \quad \frac{\alpha_1^{m'} \beta_1^{n'} \gamma_1^{p'} \ldots.}{\alpha^m \beta^n \gamma^p \ldots.} = 1.$$

Nach dem obigen Lehrsatze setzt die erstere dieser Relationen voraus, dass alle Primzahlen $\alpha_1, \beta_1, \gamma_1, \ldots.$ sich in der Reihe der Primzahlen $\alpha, \beta, \gamma, \ldots.$ vorfinden und die zweite Relation setzt umgekehrt voraus, dass alle Zahlen $\alpha, \beta, \gamma, \ldots.$ sich in der Reihe der Zahlen $\alpha_1, \beta_1, \gamma_1, \ldots.$ vorfinden; woraus folgt, dass die Zahlen $\alpha, \beta, \gamma, \ldots.$ keine anderen sind als $\alpha_1, \beta_1, \gamma_1, \ldots.$ Nehmen wir nun an, es sei

$$\alpha = \alpha_1, \quad \beta = \beta_1, \quad \gamma = \gamma_1, \ldots.,$$

so folgt, nach dem vorhergehenden Lehrsatze, aus der Gleichung

$$\frac{\alpha^m \beta^n \gamma^p \ldots.}{\alpha_1^{m'} \beta_1^{n'} \gamma_1^{p'} \ldots.} = 1,$$

dass nicht

$$m' > m; \quad n' > n; \quad p' > p, \ldots.$$

ist, während aus der Gleichung

$$\frac{\alpha_1^{m'} \beta_1^{n'} \gamma_1^{p'} \ldots.}{\alpha^m \beta^n \gamma^p \ldots.} = 1$$

umgekehrt folgt, dass nicht

$$m > m'; \quad n > n'; \quad p > p', \ldots.$$

sein kann. Aus der Vereinigung beider Gleichungen finden wir also, dass

$$m = m'; \quad n = n'; \quad p = p', \ldots.$$

sein muss. Folglich können die angenommenen zwei Zerlegungen der Zahl N weder in den einzelnen darin auftretenden Primzahlen, noch in den Potenzen, zu welchen

die betreffenden Primzahlen auftreten, sich von einander unterscheiden, wodurch die Richtigkeit des ausgesprochenen Lehrsatzes erwiesen ist.

---

§ 6. Lehrsätze, welche durch Zerlegung in Primzahlfactoren begründet werden.

Als erste Anwendung, welche wir aus der Zerlegung der Zahlen in ihre Primzahlfactoren machen, beweisen wir folgenden Lehrsatz.

6. *Lehrsatz. Ist N ein Theiler des Quadrates einer Zahl M, ohne selbst durch das Quadrat irgend einer Zahl theilbar zu sein, so ist N auch Theiler von M.*

Beweis. Indem wir die Zahl N in ihre Primzahl-Factoren zerlegen, finden wir etwa:

$$N = \alpha^m \beta^n \gamma^p \ldots .$$

Da aber N nach der Voraussetzung durch kein Quadrat irgend welcher Zahl theilbar sein darf, so können in unserem Falle die Exponenten $m, n, p, \ldots .$ die *Einheit* nicht übertreffen; denn wäre etwa nicht $m < 2$, so würde N offenbar durch α^2 theilbar sein; oder, wäre nicht $n < 2$, dann würde N durch β^2 theilbar werden, etc. Folglich sind in der vorhergehenden Gleichung alle als von Null verschieden vorausgesetzten Exponenten $m, n, p, \ldots .$ gleich 1, so dass wir erhalten:

$$N = \alpha \beta \gamma \ldots ,$$

wobei $\alpha, \beta, \gamma, \ldots .$ von einander verschiedene Primzahlen sind. Nachdem wir uns davon überzeugt haben, zerlegen wir auch die Zahl M in ihre Primzahl-Factoren und erhalten etwa:

$$M = \alpha_1^{m'} \beta^{n'} \gamma_1^{p'} \ldots ,$$

wobei $\alpha_1, \beta_1, \gamma_1, \ldots .$ von einander verschiedene Primzahlen bedeuten. Erheben wir beide Seiten dieser Gleichung zum Quadrat, so erhalten wir:

$$M^2 = \alpha_1^{2m'} \beta_1^{2n'} \gamma_1^{2p'} \ldots .$$

und indem wir uns erinnern, dass nach der Voraussetzung M^2 durch N theilbar ist, wobei

$$N = \alpha \beta \gamma \ldots .,$$

schliessen wir nach Lehrsatz 4 hieraus, dass alle Zahlen $\alpha, \beta, \gamma, \ldots .$ unter der Reihe der Zahlen $\alpha_1, \beta_1, \gamma_1, \ldots .$ sich vorfinden, und dass ihre zugehörigen Exponenten in M^2 nicht Null sind. Folglich sind alle in N enthaltenen Primzahlfactoren $\alpha, \beta, \gamma, \ldots .$ auch in M enthalten, mithin ist M durch jede der Primzahlen $\alpha, \beta, \gamma, \ldots .$ und somit (nach Lehrsatz 3) auch durch das Product derselben, nämlich durch N, theilbar, w. z. b. w.

Bemerken wir z. B., dass 15 nicht durch das Quadrat irgend einer Zahl theilbar ist, und dass 15 ein Divisor ist von 2025, welche Zahl gleich ist 45^2, so können wir daraus schliessen, dass 15 auch ein Theiler von 45 sein muss.

7. *Lehrsatz.* *Die h^{te} Wurzel einer Zahl N kann nur dann eine ganze Zahl sein, wenn alle Exponenten der in N enthaltenen Primzahlen Vielfache sind von h.*

Beweis. Die Zerlegung der Zahl N sowohl, als auch ihrer h^{ten} Wurzel in Primzahl-Factoren mag etwa ergeben:

$$N = \alpha^m \beta^n \gamma^p \ldots .$$

$$\sqrt[h]{N} = \alpha_1^{m'} \beta_1^{n'} \gamma_1^{p'} \ldots .$$

Erheben wir beide Seiten der zweiten Gleichung zur h^{ten} Potenz, so erhalten wir mit Berücksichtigung der ersten Gleichung folgende zweierlei Zerlegungen einer und derselben Zahl N in Primzahl-Factoren:

$$N = \alpha^m \beta^n \gamma^p \ldots .$$

$$N = \alpha_1^{hm'} \beta_1^{hn'} \gamma_1^{hp'} \ldots .$$

Nach Lehrsatz 5 müssen aber beide Zerlegungen mit einander identisch sein, so dass die Zahlen $\alpha, \beta, \gamma, \ldots .$ unter den Zahlen der Reihe $\alpha_1, \beta_1, \gamma_1, \ldots .$ und ebenso

die Zahlen $m, n, p, \ldots.$ unter den entsprechenden Zahlen der Reihe $hm', hn', hp', \ldots.$ ihre Gleichen haben müssen. Dieser letztere Umstand zeigt aber klar, dass die Exponenten $m, n, p, \ldots.$ gewisse Vielfache der Zahl h sind, was in unserem Lehrsatze behauptet wurde.

Finden wir z. B., dass 576 gleich ist $2^6 . 3^2$, und bemerken, dass diese Exponenten 6 und 2 den einzigen gemeinschaftlichen Theiler 2 besitzen, so können wir den Schluss ziehen, dass unter *allen möglichen* Wurzeln der Zahl 576 nur die *Quadratwurzel* allein eine ganze Zahl sein kann.

8. *Lehrsatz.* *Hat eine Zahl N bei ihrer Zerlegung in Primzahl-Factoren die Form*

$$N = \alpha^m \beta^n \gamma^p \ldots.,$$

so beträgt die Summe S aller verschiedenen Divisoren von N

$$S = \frac{\alpha^{m+1}-1}{\alpha-1} \cdot \frac{\beta^{n+1}-1}{\beta-1} \cdot \frac{\gamma^{p+1}-1}{\gamma-1} \ldots.,$$

und die Anzahl A derselben ist

$$A = (m+1)\ (n+1)\ (p+1) \ldots.$$

Beweis. Nach Lehrsatz 4 kann die Zahl N, welche dem Producte

$$\alpha^m \beta^n \gamma^p \ldots.$$

gleich ist, nur durch Zahlen von der Form

$$\alpha^{m'} \beta^{n'} \gamma^{p'} \ldots.$$

theilbar sein, wobei $m' \leqq m$; $n' \leqq n$; $p' \leqq p, \ldots.$ sein muss. Alle Divisoren der Zahl N werden daher durch alle möglichen Werthe des Productes

$$\alpha^{m'} \beta^{n'} \gamma^{p'} \ldots.,$$

welche den Werthen

$$\begin{array}{l} m' = 0,\ 1,\ 2,\ \ldots.,\ m-1,\ m; \\ n' = 0,\ 1,\ 2,\ \ldots.,\ n-1,\ n; \\ p' = 0,\ 1,\ 2,\ \ldots.,\ p-1,\ p; \\ \ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots \end{array}$$

entsprechen, bestimmt. Folglich müssen sich alle Divisoren unter der Reihe von Gliedern finden lassen, welche aus der ausgeführten Multiplication der Ausdrücke

$$(\alpha^0 + \alpha + \alpha^2 + \ldots + \alpha^{m-1} + \alpha^m),$$
$$(\beta^0 + \beta + \beta^2 + \ldots + \beta^{n-1} + \beta^n),$$
$$(\gamma^0 + \gamma + \gamma^2 + \ldots + \gamma^{p-1} + \gamma^p),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

zum Vorschein kommen. Mithin wird [*)] die Summe aller möglichen Divisoren der Zahl N durch das Product

$$(\alpha^0 + \alpha + \alpha^2 + \ldots. + \alpha^m)\ (\beta^0 + \beta + \beta^2 + \ldots. + \beta^n)$$
$$(\gamma^0 + \gamma + \gamma^2 + \ldots. + \gamma^p)\ldots.$$

vollständig bestimmt, welches, da

$$\alpha^0 + \alpha + \alpha^2 + \ldots. + \alpha^m = \frac{\alpha^{m+1}-1}{\alpha-1},$$

$$\beta^0 + \beta + \beta^2 + \ldots. + \beta^n = \frac{\beta^{n+1}-1}{\beta-1},$$

$$\gamma^0 + \gamma + \gamma^2 + \ldots. + \gamma^p = \frac{\gamma^{p+1}-1}{\gamma-1}$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

ist, das Product

$$\frac{\alpha^{m+1}-1}{\alpha-1}\cdot\frac{\beta^{n+1}-1}{\beta-1}\cdot\frac{\gamma^{p+1}-1}{\gamma-1}\ldots.,$$

ausmacht, wie im Lehrsatze behauptet wurde.

Was ferner die *Anzahl* aller Divisoren von N betrifft, so wird dieselbe durch die Anzahl der Glieder bestimmt, welche beim Ausführen der Multiplication des Productes

$$(\alpha^0 + \alpha + \alpha^2 + \ldots. + \alpha^m)$$
$$(\beta^0 + \beta + \beta^2 + \ldots. + \beta^n)$$
$$(\gamma^0 + \gamma + \gamma^2 + \ldots. + \gamma^p)\ldots.$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

erhalten werden; oder, was dasselbe ist, durch den *Werth* dieses Productes, wenn darin

[*) da offenbar auch umgekehrt jedes Glied der ausgeführten Multiplication der vorgeschriebenen Ausdrücke ein Divisor von N ist und da es ebenso klar ist, dass diese Glieder alle von einander verschieden sind,]

$$\alpha = 1, \ \beta = 1, \ \gamma = 1, \ldots .$$

gesetzt wird. Mithin ist die Anzahl aller Divisoren von N genau

$$(m+1)\,(n+1)\,(p+1)\ldots .$$

w. z. b. w.

So beträgt z. B. bei der Zahl 72, welche gleich ist $2^3 \cdot 3^2$, die Summe aller Divisoren

$$\frac{2^4-1}{2-1} \cdot \frac{3^3-1}{3-1} = 195,$$

während die Anzahl aller Divisoren von 72

$$(3+1)\,(2+1) = 12$$

ist. Von der Richtigkeit dieser Behauptungen überzeugen wir uns, indem wir bemerken, dass alle Divisoren von 72 die Zahlen

1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72,

sind, deren Summe gleich 195 und deren Anzahl 12 ist.

9. *Lehrsatz. Hat eine Zahl N bei ihrer Zerlegung in Primzahl-Factoren die Gestalt*

$$N = \alpha^m\,\beta^n\,\gamma^p \ldots,$$

wobei mindestens einer der Exponenten

$$m, n, p, \ldots .$$

eine ungerade Zahl ist, so sind für die Zahl N

$$\tfrac{1}{2}\,(m+1)\,(n+1)\,(p+1)\ldots .$$

verschiedene Zerlegungen in zwei Factoren möglich.

Sind aber sämmtliche Exponenten

$$m, n, p, \ldots .$$

gerade Zahlen, so sind für N

$$\tfrac{1}{2}\,(m+1)\,(n+1)\,(p+1)\ldots + \tfrac{1}{2}$$

Zerlegungen in je zwei Factoren möglich.

Beweis. In dem ersten Falle, wenn mindestens einer der Exponenten $m, n, p, \ldots$ ungerade ist, giebt es nach Lehrsatz 7 keine einzige Zahl, deren Quadrat gleich wäre N; mithin kann N nicht zerlegt werden in zwei Factoren,

welche einander gleich wären. Jede Zerlegung der Zahl N in zwei Factoren bestimmt somit zwei Divisoren derselben. Daraus erhellt [*)], dass die Anzahl aller möglichen Zerlegungen der Zahl N in zwei Factoren die Hälfte von der Anzahl aller Divisoren derselben ausmacht, was nach dem vorhergehenden Lehrsatze

$$\tfrac{1}{2}(m+1)(n+1)(p+1)\ldots.$$

beträgt.

In dem zweiten Falle, wenn alle Exponenten $m, n, p, \ldots.$ gerade Zahlen sind, wird unter den Zerlegungen von N in je zwei Factoren *eine* [**)] solche Zerlegung vorhanden sein, bei welcher beide Factoren einander gleich sind, so dass dieselbe nur *einen* Divisor der Zahl N bestimmt. Dann liefert aber jede der übrigen Zerlegungen, ebenso, wie im ersten Falle, je zwei Divisoren. Bezeichnet man also die gesuchte Anzahl der Zerlegungen von N in je zwei Factoren mit K, so erhält man für die Anzahl der Divisoren von N den Werth

$$1 + 2(K-1).$$

Nach dem vorhergehenden Lehrsatze ist aber die Anzahl der Divisoren von N:

$$(m+1)(n+1)(p+1)\ldots.;$$

folglich hat man:

$$1 + 2(K-1) = (m+1)(n+1)(p+1)\ldots.,$$

woraus wir für die gesuchte Zahl K den Werth

$$K = \tfrac{1}{2}(m+1)(n+1)(p+1)\ldots. + \tfrac{1}{2}$$

erhalten, was zu beweisen war.

So muss z. B. für die Zahl 72, welche gleich ist $2^3 . 3^2$,

$$K = \tfrac{1}{2}(3+1)(2+1) = 6$$

die Anzahl der Zerlegungen in zwei Factoren sein.

[*) weil offenbar auch umgekehrt zwei Zerlegungen nicht *einen* Divisor gleich haben können, ohne auch in dem *anderen* Divisor übereinzustimmen und somit als eine und dieselbe Zerlegung gezählt zu werden und folglich alle verschiedenen Zerlegungen lauter von einander verschiedene Divisoren liefern,]

[**) und offenbar *nur eine*].

Indem man die Zerlegungen von 72 in je zwei Factoren wirklich ausführt, findet man in der That, dass nur folgende 6 möglich sind:

$$1 \,.\, 72;\ \ 2 \,.\, 36;\ \ 3 \,.\, 24;\ \ 4 \,.\, 18;\ \ 6 \,.\, 12;\ \ 8 \,.\, 9.$$

Für die Zahl 36 dagegen, welche gleich ist $2^2 \,.\, 3^2$, wird die Anzahl der Zerlegungen in je zwei Factoren

$$K = \tfrac{1}{2}(2+1)(2+1) + \tfrac{1}{2} = 5.$$

In der That sind für 36 folgende 5 Zerlegungen in je zwei Factoren möglich:

$$1 \,.\, 36;\ \ 2 \,.\, 18;\ \ 3 \,.\, 12;\ \ 4 \,.\, 9;\ \ 6 \,.\, 6.$$

[Für die Zahl $1296 = 2^4 \,.\, 3^4$ sind folgende

$$\tfrac{1}{2}(4+1)(4+1) + \tfrac{1}{2} = 13$$

Zerlegungen in je zwei Factoren möglich:

$$1.1296;\ 2.648;\ 3.432;\ 6.216;\ 8.162;\ 9.144;\ 12.108;\ 16.81;\ 18.72;\ 24.54;\ 27.48;\ 36.36.]$$

---

§ 7. Ueber Zahlen, welche eine arithmetische Progression bilden.

Bevor wir weiter gehen, wollen wir noch in Bezug auf die Theilbarkeit von Zahlen, welche eine arithmetische Progression bilden, einen Satz beweisen, den wir hier und in der Folge gebrauchen werden.

10. *Lehrsatz.* *Ist in einer arithmetischen Progression aus mp Gliedern die Differenz d relativ prim zu p, so sind stets m dieser Glieder durch p theilbar.*

Beweis. Die zu betrachtende Progression mag die Gestalt haben:

$$a,\ \ a+d,\ \ a+2d, \ldots,\ \ a+(mp-2)d,\ \ a+(mp-1)d,$$

wobei d relativ prim ist zu p. Diese Reihe von Gliedern kann man in m folgende Reihen:

$$
(3)\left\{\begin{array}{lllll}
a, & a+d, & a+2d, & \ldots, & a+(p-1)d, \\
a+pd, & a+pd+d, & a+pd+2d, & \ldots, & a+pd+(p-1)d, \\
\cdot & \cdot & \cdot & & \cdot \\
a+npd, & a+npd+d, & a+npd+2d, & \ldots, & a+npd+(p-1)d, \\
\cdot & \cdot & \cdot & & \cdot \\
a+(m-1)pd, & a+(m-1)pd+d, & a+(m-1)pd+2d, & \ldots, & a+(mp-1)d
\end{array}\right.
$$

vertheilen und es ist leicht sich zu überzeugen, dass jede dieser m Reihen *ein* Glied besitzt, welches durch p theilbar ist. Um dieses einzusehen, betrachten wir unter den m Reihen die allgemeine derselben

$$a+npd,\ a+npd+d,\ a+npd+2d,\ \ldots,\ a+npd+(p-1)d,$$

in welcher n eine der Zahlen bedeutet zwischen Null und $m-1$. In dieser Reihe können nicht zwei Glieder existiren, welche nach Division derselben durch p gleiche Reste liefern sollten, weil dann die Differenz zweier solcher Glieder durch p theilbar wäre, was unmöglich ist. Denn die Differenz irgend zweier Glieder dieser Reihe ist durch ein Product $k \,.\, d$ darstellbar, wobei d, nach der Voraussetzung, relativ prim zu p ist, während für k die Bedingung besteht $k < p$, so dass diese Differenz $k \,.\, d$ nach Lehrsatz 2 durch p nicht theilbar sein kann. Sind nun die Reste, welche nach der Division der einzelnen Glieder der Reihe

$$a+npd,\ a+npd+d,\ a+npd+2d,\ \ldots,\ a+npd+(p-1)d$$

durch p erhalten werden, alle von einander verschieden, so dass nicht mehr als *ein* solcher Rest der Null gleich sein kann, so wird andererseits *einer* dieser Reste unbedingt Null sein müssen. Denn würden wir das Gegentheil annehmen, und bemerken, dass für die Reste, welche eine Zahl überhaupt nach der Division derselben durch p liefern kann, ausser der Null nur noch die $p-1$ möglichen Werthe

$$1,\ 2,\ 3,\ \ldots,\ p-1$$

übrig bleiben, so würden wir zugeben müssen, dass unter den p Resten, welche die p Glieder der Reihe

$$a+npd,\ a+npd+d,\ a+npd+2d,\ \ldots,\ a+npd+(p-1)d$$

nach ihrer Division durch p liefern, mindestens zwei einander gleich seien, was nach dem oben Bewiesenen unmöglich ist.

Haben wir uns auf diese Weise überzeugt, dass in der *allgemeinen* Reihe

$$a+npd,\ a+npd+d,\ a+npd+2d,\ \ldots,\ a+npd+(p-1)d$$

und folglich in *jeder* Reihe des Reihensystems (3) die Anzahl derjenigen Glieder, welche durch p theilbar sind gleich 1 ist, so schliessen wir, dass in allen m Reihen (3) zusammen genau m Glieder durch p theilbar sind. Die Gesammtheit der Reihen (3) stellt aber, wie wir gesehen haben, die von uns betrachtete Progression aus mp Gliedern

$$a,\ a+d,\ a+2d,\ \ldots,\ a+(mp-2)d,\ a+(mp-1)d$$

dar, und so folgt daraus die Richtigkeit unseres Satzes.

Aus diesem Satze lässt sich ohne Schwierigkeit folgender Lehrsatz herleiten:

11. *Lehrsatz.* *Ist a eine Primzahl und A relativ prim zu a, so verhält sich in der Reihe der Zahlen*

$$1, 2, 3, \ldots, aAN-1, aAN$$

die Anzahl derjenigen ihrer Glieder, welche relativ prim sind zu A, zur Anzahl solcher Glieder, welche zugleich zu A und zu a relativ prim sind, wie a zu $a-1$ [*)].

Beweis. In der Arithmetik wird bewiesen, dass der grösste gemeinschaftliche Theiler zweier Zahlen X und A zugleich auch der grösste gemeinschaftliche Theiler ist von A und von dem Reste, welcher nach Division von X

[*) Bezeichnet man die Anzahl derjenigen Glieder der genannten Reihe, welche relativ prim sind zu A, etwa mit $\mathfrak{A}$ und die Anzahl derjenigen, welche zu A und zu a relativ prim sind, mit $\mathfrak{a}$, so ist

$$\mathfrak{A} : \mathfrak{a} = a : (a-1)].$$

durch A erhalten wird [*)]. Daraus folgt, dass wenn X und A *keinen* gemeinschaftlichen Theiler besitzen, dann auch der Rest bei der Division von X durch A ebenfalls relativ prim zu A sein muss und umgekehrt; ist der Rest bei der Division von X durch A relativ prim zu A, so ist auch X relativ prim zu A. Weil aber der Rest bei der Division irgend einer Zahl durch A immer kleiner sein muss als A, so wird der Rest der Division von X durch A, wenn X relativ prim ist zu A, immer eine der Zahlen sein, welche kleiner als A und relativ prim sind zu A. Mögen nun

$$\alpha', \alpha'', \alpha''', \ldots., \alpha^{(n)}$$

die Zahlen sein, welche kleiner als A und relativ prim zu A sind; dann ist es leicht die Gestalt einer Zahl X so zu bestimmen, dass der Rest der Division derselben durch A einer der Zahlen $\alpha', \alpha'', \alpha''', \ldots., \alpha^{(n)}$ gleich werde. Damit z. B. eine Zahl X nach Division durch A den Rest α' liefere, bezeichnen wir den Quotienten der Division von X durch A mit m' und erhalten für X, indem wir den Dividendus der Summe des Productes von Divisor und Quotienten plus dem Reste gleich setzen, folgende Formel:

$$X = \alpha' + m'A.$$

Ebenso finden wir für die Zahlen, welche nach Division durch A die Reste $\alpha'', \alpha''', \ldots., \alpha^{(n)}$ liefern die analogen Formeln:

$$X = \alpha'' + m'''A;\ \ X = \alpha''' + m'''A;\ \ \ldots.;\ \ X = \alpha^{(n)} + m^{(n)}A.$$

Mithin werden alle Zahlen, welche nach Division durch A die Reste $\alpha', \alpha'', \alpha''', \ldots. \alpha^{(n)}$ liefern und somit nach dem oben Bemerkten relativ prim zu A sind, in der Form

$$X = \alpha' + m'A;\ \ X = \alpha'' + m''A;\ \ X = \alpha''' + m'''A;\ \ \ldots.;\ \ X = \alpha^{(n)} + m^{(n)}A$$

[*) Der Beweis hierfür erfordert bekanntlich nur die Bildung eines Systems von Gleichungen, das dem bei Lehrsatz 1 pag. 6, aufgestellten ähnlich ist und durch die wirkliche successive Division zwischen X, A und den aufeinanderfolgenden Resten entsteht. Es wird dann der letzte Rest r_n der grösste gemeinschaftliche Theiler, woraus die obige Behauptung unmittelbar erhellt.]

dargestellt werden. Mit Hülfe dieser Formeln können wir nunmehr leicht die Richtigkeit unseres Lehrsatzes beweisen.

Zu dem Ende bestimmen wir nach diesen Formeln alle Zahlen, welche kleiner als aAN und relativ prim zu A sind, indem wir den Grössen $m', m'', m''', \ldots, m^{(n)}$ die Werthe 0, 1, 2, 3, etc. beilegen und zwar so lange fortgesetzt, als nur die durch diese Formeln bestimmten Zahlen die Zahl aAn nicht übertreffen.

Auf diese Weise finden wir, dass alle Zahlen, welche kleiner als aAN und relativ prim zu A sind, durch die Zahlen

$$\begin{array}{l}
\alpha', \ \alpha' + A, \ \alpha' + 2A, \ \ldots, \ \alpha' + (aN-1)A, \\
\alpha'', \ \alpha'' + A, \ \alpha'' + 2A, \ \ldots, \ \alpha'' + (aN-1)A, \\
\alpha''', \ \alpha''' + A, \ \alpha''' + 2A, \ \ldots, \ \alpha''' + (aN-1)A, \\
\ldots\ldots\ldots\ldots\ldots\ldots \\
\alpha^{(n)}, \ \alpha^{(n)} + A, \ \alpha^{(n)} + 2A, \ \ldots, \ \alpha^{(n)} + (aN-1)A
\end{array}$$

repräsentirt werden, deren Anzahl, wie man leicht ersieht, genau aNn beträgt.

Jetzt ist es aber auch leicht die Anzahl derjenigen Zahlen zu bestimmen, welche kleiner als aAN und relativ prim sind zu A und zu a. Dazu genügt es, unter den ebengefundenen Zahlen, welche relativ prim zu A sind, die Vielfachen von a, auszuscheiden; denn, da a, nach Voraussetzung, Primzahl ist, so sind alle durch a nicht theilbaren Zahlen, nach § 3, relativ prim zu a. Nach dem vorhergehenden Lehrsatze sind aber unter den aN Gliedern der Reihe

$$\alpha', \ \alpha' + A, \ \alpha' + 2A, \ \alpha' + 3A, \ \ldots, \ \alpha' + (aN-1)A,$$

N Glieder enthalten, welche durch a theilbar sind; folglich ist in diesem Falle die Anzahl derjenigen Glieder, welche zu a relativ prim sind, $aN - N$, oder $(a-1)N$. Dasselbe bemerken wir bei den übrigen Reihen:

$$\begin{array}{l}
\alpha'', \ \alpha'' + A, \ \alpha'' + 2A, \ \ldots, \ \alpha'' + (aN-1)A, \\
\alpha''', \ \alpha''' + A, \ \alpha''' + 2A, \ \ldots, \ \alpha''' + (aN-1)A, \\
\ldots\ldots\ldots\ldots\ldots\ldots \\
\alpha^{(n)}, \ \alpha^{(n)} + A, \ \alpha^{(n)} + 2A, \ \ldots, \ \alpha^{(n)} + (aN-1)A.
\end{array}$$



Daraus folgt, dass die Anzahl aller Zahlen, die kleiner als aAn und relativ prim sind zu A und a, gleich ist $(a-1)Nn$. Folglich verhält sich diese Anzahl zu der oben gefundenen Anzahl aAn aller Zahlen, die kleiner als aAN und relativ prim zu A sind, wie $(a-1)$ zu a [*)], was wir beweisen wollten.

Mit Hülfe der oben bewiesenen Lehrsätze, sind wir nun im Stande folgenden Lehrsatz zu beweisen.

12. *Lehrsatz.* *Hat eine Zahl N bei Zerlegung in Primzahlfactoren die Gestalt*

$$N = \alpha^m \beta^n \gamma^p \ldots . \pi^r,$$

so stellt

$$\alpha^m \beta^n \gamma^p \ldots . \pi^r . \frac{\alpha-1}{\alpha} . \frac{\beta-1}{\beta} . \frac{\gamma-1}{\gamma} \ldots . \frac{\pi-1}{\pi}$$

die Anzahl aller Zahlen dar, welche kleiner als N und relativ prim zu N sind [**)].

Beweis. Mit Hülfe der vorhergehenden Lehrsätze kann man leicht zeigen, wie viel Zahlen es in der Reihe

$$1, 2, 3, \ldots ., \alpha^m \beta^n \gamma^p \ldots . \pi^r$$

giebt, welche zugleich relativ prim sind zu α, zu β, zu γ, ... und zu π. Zu diesem Zwecke schreiben wir diese Reihe in Gestalt einer arithmetischen Progression mit der Differenz 1, und zwar so:

$$1, 1+1, 1+2.1, \ldots ., 1+(\alpha\, \alpha^{m-1} \beta^n \gamma^p \ldots . \pi^r - 1).$$

Nach Lehrsatz 10 schliessen wir, dass die Anzahl derjenigen Glieder dieser Reihe, welche durch α theilbar sind,

---

[*) Bezeichnen wir also unter den Zahlen, welche kleiner als aAn sind, die Anzahl derjenigen, welche zu A und a relativ prim sind, mit $\mathfrak{a}$ und die Anzahl derjenigen, die nur zu A relativ prim sind, mit $\mathfrak{A}$, so ist $\mathfrak{A} = aNn$; $\mathfrak{a} = (a-1)Nn$, also: $\mathfrak{A} : \mathfrak{a} = a : (a-1)$].

[**) Bezeichnet man also, wie nach *Gauss* in der Zahlentheorie üblich geworden, die Anzahl aller Zahlen, welche kleiner als eine Zahl N und relativ prim zu N sind, mit $\varphi(N)$ und ist $N = \alpha^m \beta^n \gamma^p \ldots . \pi^r$, so ist immer

$$\varphi(N) = N \frac{\alpha-1}{\alpha} \frac{\beta-1}{\beta} \frac{\gamma-1}{\gamma} \ldots . \frac{\pi-1}{\pi}].$$

$\alpha^{m-1}\,\beta^n\,\gamma^p\ldots.\pi^r$ sein wird[*)], und somit werden alle übrigen Glieder dieser Reihe, deren Anzahl

$$\alpha^m\,\beta^n\,\gamma^p\ldots.\pi^r - \alpha^{m-1}\,\beta^n\,\gamma^p\ldots.\pi^r = \alpha^m\,\beta^n\,\gamma^p\ldots.\pi^r\,.\,\frac{\alpha-1}{\alpha}$$

ist, relativ prim sein zu α (s. § 3). In der Reihe

$$1, 2, 3, \ldots., \alpha^m\,\beta^n\,\gamma^p\ldots.\pi^r$$

sind also genau

$$\alpha^m\,\beta^n\,\gamma^p\ldots.\pi^r\,.\,\frac{\alpha-1}{\alpha}$$

Glieder relativ prim zu α.

Daraus folgt nach Lehrsatz 11, dass die Anzahl der Glieder, welche zugleich relativ prim sind zu α und zu β, oder, was dasselbe ist, zum Producte $\alpha\beta$, genau

$$\alpha^m\,\beta^n\,\gamma^p\ldots.\pi^r\,.\,\frac{\alpha-1}{\alpha}\,.\,\frac{\beta-1}{\beta}$$

beträgt[**)]. Wissen wir nun, dass in der Reihe

$$1, 2, 3, \ldots., \alpha^m\,\beta^n\,\gamma^p\ldots.\pi^r$$

die Anzahl der Glieder, welche relativ prim zu der Zahl $\alpha\beta$ sind,

$$\alpha^m\,\beta^n\,\gamma^p\ldots.\pi^r\,.\,\frac{\alpha-1}{\alpha}\,.\,\frac{\beta-1}{\beta}$$

beträgt, so schliessen wir ferner daraus nach demselben Lehrsatz 11, [indem man dort $A = \alpha\beta$ und $a = \gamma$ setzt], dass in derselben Reihe die Anzahl der Glieder, welche relativ prim sind zu $\alpha\beta\gamma$ genau

$$\alpha^m\,\beta^n\,\gamma^p\ldots.\pi^r\,.\,\frac{\alpha-1}{\alpha}\,.\,\frac{\beta-1}{\beta}\,.\,\frac{\gamma-1}{\gamma}$$

beträgt; u. s. w. Auf diese Weise finden wir endlich, dass die Anzahl der Glieder, welche relativ prim sind zu $\alpha\beta\gamma\ldots.\pi$ genau

---

[*) Man braucht nur in Lehrsatz 10 die Werthe $p = \alpha$ und $m = \alpha^{m-1}\,\beta^n\,\gamma^p\ldots.\pi^r$ einzusetzen].

[**) Man braucht nur in Lehrsatz 11 in der Formel $\mathfrak{A} : \mathfrak{a} = a : (a-1)$, oder $\mathfrak{a} = \mathfrak{A}\,\frac{a-1}{a}$ die Werthe $A = \alpha$; $a = \beta$ zu setzen].

$$\alpha^m \beta^n \gamma^p \dots \pi^r . \frac{\alpha-1}{\alpha} . \frac{\beta-1}{\beta} . \frac{\gamma-1}{\gamma} \dots \frac{\pi-1}{\pi}$$

beträgt.

Somit haben wir die Anzahl der Zahlen, welche relativ prim zu $\alpha\beta\gamma \dots \pi$ und kleiner als $\alpha^m\beta^n\gamma^p \dots \pi^r$ sind, bestimmt. Es ist aber dieses vollkommen gleichbedeutend mit der Anzahl derjenigen Zahlen, welche relativ prim sind zu N, oder, was dasselbe ist, zu $\alpha^m \beta^n \gamma^p \dots \pi^r$, die wir eigentlich suchen; weil alle Zahlen, welche zu $\alpha^m\beta^n\gamma^p \dots \pi^r$ relativ prim sind, auch relativ prim zu $\alpha\beta\gamma \dots \pi$ sein müssen und umgekehrt. Davon überzeugen wir uns durch den Umstand, dass sowohl zu $\alpha^m \beta^n \gamma^p \dots \pi^r$, als auch zu $\alpha\beta\gamma \dots \pi$ irgend eine Zahl relativ prim sein wird, wenn in ihren Bestandtheilen keine der Zahlen $\alpha, \beta, \gamma, \dots, \pi$ als Factor vorkommt und im entgegengesetzten Falle wird dieselbe weder zu $\alpha^m \beta^n \gamma^p \dots \pi^r$, noch zu $\alpha\beta\gamma \dots \pi$ relativ prim sein.

Es giebt also wirklich der Ausdruck

$$\alpha^m \beta^n \gamma^p \dots \pi^r \frac{\alpha-1}{\alpha} . \frac{\beta-1}{\beta} . \frac{\gamma-1}{\gamma} \dots \frac{\pi-1}{\pi}$$

genau an, wie viele unter den Gliedern der Reihe

$$1, 2, 3, \dots, \alpha^m \beta^n \gamma^p \dots \pi^r$$

relativ prim sind zu $\alpha^m \beta^n \gamma^p \dots \pi^r$, was bewiesen werden sollte.

Um z. B. zu erfahren wie viel Zahlen kleiner als 36 und relativ prim zu 36 sind, zerlegen wir 36 in Primzahlfactoren. Indem wir nun finden, dass $36 = 2^2 . 3^2$ ist, schliessen wir nach unserem bewiesenen Lehrsatze, dass die Anzahl aller Zahlen, welche kleiner als 36 und relativ prim zu 36 sind, genau

$$2^2 . 3^2 \frac{2-1}{2} . \frac{3-1}{3} = 12$$

beträgt. In der That finden wir unter allen Zahlen von 1 bis 36 folgende 12 Zahlen

1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35,

die relativ prim sind zu 36; alle übrigen 23 Zahlen

2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 26,
27, 28, 30, 32, 33, 34,

besitzen mit 36 gemeinschaftliche Theiler.

Hiermit schliessen wir nun die Auseinandersetzung derjenigen Eigenschaften der Zahlen, welche für die Begründung des Folgenden nothwendig sind und gehen nunmehr zu der Untersuchung der Congruenzen über.

Kapitel I.

Ueber Congruenzen im Allgemeinen.

§ 8. Ueber den Begriff einer Congruenz.

Die *Theorie der Congruenzen* hat zum Gegenstand ihrer Untersuchungen diejenigen unbestimmten Gleichungen, welche eine der Unbekannten in der ersten Potenz enthalten. Die allgemeine Gestalt solcher Gleichungen ist

$$F(x, y, z, \ldots.) = Au + B,$$

wobei F eine gegebene Function bedeutet und A, wie B bestimmte Zahlen sind. Da solche Gleichungen sehr oft gebraucht werden, so hat man für dieselben eine besondere Bezeichnung eingeführt, welche auf folgender Betrachtung beruht. Es ist nämlich leicht zu bemerken, dass, bei der Unbestimmtheit des Werthes der Zahl u, die Gleichung

$$F(x, y, z, \ldots.) = Au + B,$$

auf die Form

$$\frac{F(x, y, z, \ldots.) - B}{A} = u$$

gebracht, nichts Anderes besagt, als die Theilbarkeit der Differenz $F(x, y, z, \ldots.) - B$ durch A. Man kann daher diese Gleichung auch so schreiben:

$$F(x, y, z, \ldots.) \equiv B \text{ (Mod. } A),$$

indem man nämlich ein für alle Mal mit dem Zeichen $\equiv$, welches zwischen zwei Zahlen gesetzt wird, die Theilbar-

keit der Differenz dieser Zahlen durch eine dritte Zahl, welche letztere mit voranstehendem Worte Mod. [Abkürzung von *„modulo“*] in runden Klammern beigesetzt wird, ausdrückt.

So werden wir z. B., um die Theilbarkeit der Differenz $17-5$ durch 3 auszudrücken, es so schreiben:

$$17 \equiv 5 \pmod{3}.$$

Ausdrücke von dieser Gestalt:

$$M \equiv N \pmod{A}$$

sind nun bekannt unter dem Namen „Congruenzen“, die Zahlen M und N nennt man „einander congruent“ nach dem Modul A, die Zahl A heisst „der Modul der Congruenz.“ [Man drückt damit aus, dass die Differenz beider Zahlen M und N nach Division durch A den Rest Null liefert. Hat man anstatt einer Zahl M die Zahl N gesetzt, so hat man einen Fehler von $M-N$ gemacht. Kommt es jedoch bei einer gewissen Aufgabe nicht auf die Zahl selbst, sondern nur auf ihren Rest an, welchen man erhält nach der Division derselben durch A, so hat man durch ein solches Ersetzen von M durch N gar keinen Fehler verursacht, wenn die Differenz $M-N$ nach Division durch A überhaupt keinen Rest giebt. Es ist also in solchem Falle *gleichgültig*, ob man M oder N nimmt. Diese Aequivalenz von M und N in Bezug auf ihre Theilbarkeit durch A ist es also, welche man mit dem Ausdrucke: „M und N sind einander congruent, oder M ist congruent N nach dem Modul A“ aussagen will]. Uebrigens können die Zahlen, deren Congruenz behauptet wird, positiv oder negativ sein; in allen Fällen bedeutet der Ausdruck

$$M \equiv N \pmod{A}$$

die Theilbarkeit der [sogenannten] algebraischen Differenz $M-N$ durch A. Die Zahl A, d. h. den Modul der Congruenz, werden wir dagegen immer positiv voraussetzen.

Wir bemerken zunächst, dass nach der eben auseinandergesetzten Bezeichnung immer

$$M \equiv r \pmod{A}$$

sein wird, wenn r der Rest der Division von M durch A ist; denn bezeichnen wir mit q den Quotienten der Division von M durch A und setzen den Dividendus gleich der Summe des Productes von Divisor und Quotienten plus dem Reste, so erhalten wir

$$M = Aq + r,$$

woraus sofort erhellt, dass die Differenz von M und r durch A theilbar ist.

Es ist nicht schwer sich auch von der Richtigkeit der Umkehrung zu überzeugen; nämlich, dass, wenn bei positiven M und r die Zahl r kleiner als A und congruent ist M nach dem Modul A, dann r der Rest der Division von M durch A sein muss. Denn aus der Congruenz

$$M \equiv r \pmod{A}$$

folgt

$$\frac{M-r}{A} = q,$$

wobei q irgend eine ganze Zahl ist; mithin ist

$$M = Aq + r;$$

und diese Gleichung stellt, bei $r < A$ und $r \geqq 0$, die Zahl r als Rest der Division von M durch A dar.

Aus dem Umstande nun, dass der Dividendus immer congruent ist dem Reste, wenn der Divisor als Modul genommen wird, folgern wir als speciellen Fall, dass wenn M durch A ohne Rest theilbar ist, dann

$$M \equiv 0 \pmod{A}$$

sein wird.

Aus diesem Grunde werden wir häufig sagen:

„eine Zahl sei congruent Null nach dem Modul A“,

anstatt zu sagen:

die Zahl ist durch A theilbar.

---

§ 9. Ueber die Eigenschaften der Congruenzen von Zahlen.

Aus dem auseinandergesetzten Begriffe von Congruenzen ist es nun leicht folgende Eigenschaften derselben direct herzuleiten:

1. *Zwei Zahlen, welche einer und derselben dritten Zahl nach irgend einem Modul congruent sind, sind auch nach demselben Modul unter einander congruent.*

Sind

$$M \equiv N \ (\text{mod. } A),$$
$$M' \equiv N \ (\text{mod. } A),$$

so muss auch in der That

$$M \equiv M' \ (\text{mod. } A)$$

sein.

Denn die Congruenzen $M \equiv N$ (mod. A) und $M' \equiv N$ (mod. A) setzen die Theilbarkeit von $M-N$ und $M'-N$ durch A voraus; folglich ist A auch ein Theiler der Differenz dieser Differenzen, d. h. von $M-M'$. Die Theilbarkeit dieser letzten Differenz $M-M'$ durch A wird aber durch die Congruenz

$$M \equiv M' \ (\text{mod. } A)$$

ausgedrückt.

2. *In ähnlicher Weise wie bei Gleichungen, können auch bei Congruenzen die Glieder von der einen Seite nach der anderen (mit umgekehrten Vorzeichen) geschafft werden.*

Ist z. B.

$$M + M' \equiv N \ (\text{mod. } A),$$

so ist auch

$$M \equiv N - M' \ (\text{mod. } A).$$

In der That drückt die Congruenz $M + M' \equiv N$ (mod. A) aus, dass $M + M' - N$ durch A theilbar ist. Die Grösse $M + M' - N$ kann man aber auch so als Differenz schreiben: $M-(N-M')$ und die Theilbarkeit dieser Differenz durch A wird durch die Congruenz $M \equiv N - M'$ (mod. A) ausgedrückt.

3. *Zwei oder mehrere Congruenzen mit einem und demselben Modul können gliedweise zu einander addirt oder von einander subtrahirt werden.*

Sind nämlich

$$M \equiv N \text{ (mod. A)},$$
$$M' \equiv N' \text{ (mod. } A),$$

so ist auch

$$M \pm M' \equiv N \pm N' \text{ (mod. } A).$$

Davon überzeugt man sich leicht, wenn man bemerkt, dass die Congruenzen $M \equiv N$ (mod. A); $M' \equiv N'$ (mod. A) die Theilbarkeit der Differenzen $M - N$, resp. $M' - N'$ durch A voraussetzen. Daraus folgt aber die Theilbarkeit von $M - N \pm (M' - N')$ oder, was dasselbe ist, von $M \pm M' - (N \pm N')$ durch A; die Theilbarkeit von $M \pm M' - (N \pm N')$ durch A drückt man aber durch die Congruenz $M \pm M' \equiv N \pm N'$ (mod. A) aus, was wir beweisen wollten.

Von der Vereinigung zweier Congruenzen ist es nun leicht zu einer Vereinigung von drei, vier und mehr solcher überzugehen.

4. *Die Glieder einer Congruenz können mit einer und derselben Zahl multiplicirt werden.*

Besteht also die Congruenz

$$M \equiv N \text{ (mod. } A),$$

so ist auch

$$k\,.\,M \equiv k\,.\,N \text{ (mod. } A).$$

In der That erhalten wir, indem wir auf Grund der vorhergehenden Eigenschaft, k gleichlautende Congruenzen $M \equiv N$ (mod. A) gliedweise zu einander addiren, als Resultat: $kM \equiv kN$ (mod. A), wodurch die Berechtigung, die Glieder einer Congruenz mit einer beliebigen ganzen *positiven* Zahl zu multipliciren, bewiesen ist. Was nun das Multipliciren mit einer *negativen* Zahl betrifft, so bemerken wir, dass wenn $kM \equiv kN$ (mod. A) ist, so ist auch $-kM \equiv -kN$ (mod. A); denn die erstere Congruenz sagt aus, dass die Zahl $kM - kN$ durch A theilbar ist; dann ist aber auch noch dieselbe, mit negativen Vorzeichen genommene Zahl, d. h. $-kM + kN$ durch A theilbar. Die Theilbarkeit dieser letzteren drückt man nun durch die Congruenz $-kM \equiv -kN$ (mod. A) aus.

[Letzteres kann auch mit Hülfe von Eigenschaft (2) bewiesen werden; oder auch auf Grund von (3) und zwar in derselben Weise wie für ein positives k, indem man nämlich zuerst $k+1$ gleiche Congruenzen zu einander addirt und dann die Summe von der ursprünglichen subtrahirt. Uebrigens ist oben § 8 bei der Erklärung des Begriffes der Congruenz bereits gesagt worden: es dürfen die Zahlen M und N auch negativ sein und es sei überhaupt immer von einer *algebraischen* Differenz die Rede.]

5. *Zwei oder mehrere Congruenzen mit einem und demselben Modul können gliedweise mit einander multiplicirt werden.*

Bestehen nämlich die Congruenzen

$$\begin{aligned} M &\equiv N \pmod{A} \\ M' &\equiv N' \pmod{A} \\ M'' &\equiv N'' \pmod{A}, \\ &\vdots \end{aligned}$$

so ist auch

$$M\,M'\,M'' \ldots\ldots \equiv N\,N'\,N'' \ldots\ldots \pmod{A}.$$

In der That drücken die ersten zwei Congruenzen $M \equiv N \pmod{A}$ und $M' \equiv N' \pmod{A}$ die Theilbarkeit der Zahlen $M-N$ und $M'-N'$ durch A aus. Bezeichnet man die Quotienten bei diesen Divisionen mit q, resp. q', so erhält man

$$\frac{M-N}{A} = q, \quad \frac{M'-N'}{A} = q',$$

woraus folgt:

$$M = Aq + N, \quad M' = Aq' + N'.$$

Multiplicirt man diese Gleichungen mit einander, so erhält man die Gleichung

$$MM' = A^2qq' + A(qN' + q'N) + NN',$$

oder

$$MM' - NN' = A^2qq' + A(qN' + q'N),$$

welche die Theilbarkeit der Differenz $MM' - NN'$ durch A aussagt, und folglich gleichbedeutend ist mit der Congruenz

$$MM' \equiv NN' \pmod{A}.$$

Multipliciren wir dieses gliedweise Product der ersten zwei Congruenzen wiederum gliedweise mit den Gliedern der dritten Congruenz $M'' \equiv N'' \pmod{A}$ und so fort, so gelangen wir zu der Congruenz

$$MM'M''\ldots. \equiv NN'N''\ldots. \pmod{A}.$$

Corollar. Nehmen wir speciell an, es sei:

$$M = M' = M'' = \ldots.;$$
$$N = N' = N'' = \ldots.$$

und bezeichnen mit k die Anzahl der gleichen Zahlen M, M', M'',.... und N, N', N''...., so finden wir noch, dass man aus der Congruenz

$$M \equiv N \pmod{A}$$

immer

$$M^k \equiv N^k \pmod{A}$$

folgern kann.

Auf Grund dieser Eigenschaften können wir nun folgenden allgemeinen Satz aussprechen:

6. *Die Werthe einer ganzen Function mit ganzen Coëfficienten von zwei Zahlen, welche nach irgend einem Modul congruent sind, sind selbst nach demselben Modul einander congruent.*

Ist nämlich

$$M \equiv N \pmod{A}$$

und bedeutet $f(x)$ eine ganze Function von x, etwa

$$f(x) = ax^m + bx^{m-1} + cx^{m-2} + \ldots. + px + q,$$

wobei $a, b, c, \ldots. p, q$ und m ganze Zahlen sind, so ist auch

$$f(M) \equiv f(N) \pmod{A}.$$

In der That folgen nach dem eben Bewiesenen, aus

$$M \equiv N \pmod{A}$$

die Congruenzen

$$M^m \equiv N^m;\quad M^{m-1} \equiv N^{m-1};\quad M^{m-2} \equiv N^{m-2};\ \ldots. \pmod{A},$$



woraus wir durch beziehungsweise Multiplication mit a, b, c, ... erhalten:

$$\left.\begin{array}{lcl} aM^m & \equiv & aN^m \\ bM^{m-1} & \equiv & bN^{m-1} \\ cM^{m-2} & \equiv & cN^{m-2} \\ & \vdots & \\ pM & \equiv & pN \\ q & \equiv & q \end{array}\right\} \text{(mod. } A).$$

Addirt man die letzterhaltenen Congruenzen gliedweise und bezeichnet:

$$aM^m + bM^{m-1} + cM^{m-2} + \ldots + pM + q = f(M),$$
$$aN^m + bN^{m-1} + cN^{m-2} + \ldots + pN + q = f(N),$$

so erhält man

$$f(M) \equiv f(N) \text{ (mod. } A),$$

was wir beweisen wollten.

7. *Die Glieder einer Congruenz können durch einen etwaigen gemeinschaftlichen Factor derselben gekürzt (dividirt) werden, wenn ein solcher Factor relativ prim ist zum Modul der Congruenz.*

Ist also

$$kM \equiv kN \text{ (mod. } A),$$

wobei k relativ prim ist zu A, so ist auch

$$M \equiv N \text{ (mod. } A).$$

In der That setzt die Congruenz $kM \equiv kN$ (mod. A) die Theilbarkeit von $kM - kN$, oder $k(M - N)$ durch A voraus. Darin ist aber, wenn k relativ prim zu A ist, nach Lehrsatz 2, die Voraussetzung der Theilbarkeit von $M - N$ durch A enthalten, welche durch die Congruenz $M \equiv N$ (mod. A) ausgedrückt wird.

8. *Ist eine Seite einer Congruenz und der Modul derselben durch eine und dieselbe Zahl theilbar, so muss auch die andere Seite der Congruenz durch dieselbe*

Zahl theilbar sein, wenn die Congruenz überhaupt möglich sein soll.

Ist nämlich die Congruenz

$$M \equiv kN \pmod{kA}$$

gegeben, so muss M durch k theilbar sein, wenn die Congruenz richtig sein soll.

Die gegebene Congruenz sagt nämlich, dass die Differenz $M - kN$ durch kA theilbar ist. Bezeichnet man nun mit q den Quotienten dieser Division, so erhält man

$$\frac{M - kN}{kA} = q,$$

woraus folgt:

$$M = k(N + Aq),$$

wodurch die Theilbarkeit von M durch k erhellt.

9. *Ein gemeinschaftlicher Factor der Glieder einer Congruenz und des Moduls derselben kann weggelassen werden.*

Ist also

$$kM \equiv kN \pmod{kA},$$

so ist auch

$$M \equiv N \pmod{A}.$$

Die Congruenz $kM \equiv kN \pmod{kA}$ sagt nämlich die Theilbarkeit von $kM - kN$ durch kA aus; aber die Zahl

$$\frac{kM - kN}{kA} = q$$

kann auf die Form

$$\frac{M - N}{A} = q$$

zurückgeführt werden. Die Theilbarkeit von $M - N$ durch A wird aber durch die Congruenz

$$M \equiv N \pmod{A}$$

ausgedrückt.

10. *Zwei oder mehrere Zahlen, welche unter einander congruent sind in Bezug auf mehrere Moduln, die relativ prim zu einander sind, sind auch congruent in Bezug auf das Product dieser Moduln.*

Sind z. B. die Congruenzen

$$M \equiv N \,(\text{mod.}\, A)$$
$$M \equiv N \,(\text{mod.}\, A')$$

gegeben, wobei A, A' relative Primzahlen sind, so ist auch

$$M \equiv N \,(\text{mod.}\, A \,.\, A').$$

Denn in den Congruenzen $M \equiv N \,(\text{mod.}\, A)$ und $M \equiv N \,(\text{mod.}\, A')$ wird ausgesagt, dass die Differenz $M - N$ sowohl durch A als durch A' theilbar ist. Sind aber A und A' relativ prim zu einander, so ist in dieser Theilbarkeit durch A und A', nach Lehrsatz 3, die Theilbarkeit durch das Product $A\,A'$ enthalten, was man durch die Congruenz $M \equiv N \,(\text{mod.}\, A\,A')$ ausdrückt.

Hat man nun mehrere Congruenzen

$$M \equiv N \,(\text{mod.}\, A),\; M \equiv N \,(\text{mod.}\, A'),\; M \equiv N \,(\text{mod.}\, A''), \ldots,$$

wobei alle Zahlen $A, A', A'', \ldots$ unter einander relativ prim sind, so findet man zunächst, durch die Vereinigung der ersten zwei Congruenzen: $M \equiv N \,(\text{mod.}\, A\,A')$; durch Vereinigung dieser letzteren mit $M \equiv N \,(\text{mod.}\, A'')$ erhalten wir dann $M \equiv N \,(\text{mod.}\, A\,A'\,A'')$ u. s. w., worin die ausgesprochene Eigenschaft enthalten ist[*)].

11. *Ohne die Richtigkeit einer Congruenz zu beeinträchtigen, kann man den Modul derselben durch jede Zahl ersetzen, durch welche derselbe theilbar ist.*

So ist z. B., wenn

$$M \equiv N \;(\text{mod.}\, A\,A')$$

gegeben ist, auch

$$M \equiv N \;(\text{mod.}\, A).$$

Multiplicirt man in der That (nach 4) beide Seiten der gegebenen Congruenz mit A', so erhält man

$$A'\,M \equiv A'\,N \;(\text{mod.}\, A'\,A).$$

Nach der obenerwähnten Eigenschaft (Nr. 9) der Congruenzen

[*) Es folgt diese Erweiterung für mehrere Congruenzen auch direct aus dem erweiterten Lehrsatz 3].

kann ein gemeinschaftlicher Factor in beiden Seiten der Congruenz und im Modul zu gleicher Zeit stets weggelassen werden. Lässt man nun in $A'M \equiv A'N \pmod{A'A}$ den Factor A' überall weg, so erhält man $M \equiv N \pmod{A}$, w. z. b. w. [*)].

Dieses sind nun die Haupteigenschaften von Congruenzen je zweier Zahlen unter einander, welche uns zur Lösung solcher Congruenzen dienen werden, die eine oder mehrere Unbekannte enthalten. Zu dieser Lösung wollen wir jetzt übergehen.

---

§ 10. **Ueber die Lösung von Congruenzen.**

Wir haben gesehen, dass die Glieder einer Congruenz von der einen Seite derselben nach der anderen geschafft werden können. Denken wir uns alle Glieder nach einer Seite der Congruenz geschafft, so haben wir dieselbe auf die Gestalt

$$f(x, y, z, \ldots) \equiv 0 \pmod{p}$$

zurückgeführt, wobei f irgend eine Function, p eine gegebene Zahl, welche als Modul angenommen wird und $x, y, z, \ldots$ unbekannte Zahlen bedeuten.

Wir werden unsere Untersuchungen mit den einfachsten Congruenzen beginnen; mit solchen, nämlich, welche nur *eine* Unbekannte enthalten, und wollen zunächst den Fall betrachten, in dem die in der Congruenz vorkommende Function eine *ganze, mit ganzzahligen Coëfficienten* ist.

Indem wir uns auf Congruenzen solcher Art beschränken, beweisen wir für dieselben folgenden

---

[*) Der Beweis ist mit Absicht so geführt, um eine Anwendung der obigen Eigenschaften zu veranlassen; man kann aber offenbar die Richtigkeit dieser Eigenschaft, wie dieses bei den obigen Eigenschaften oft geschehen ist, auch direct so zeigen: Die Congruenz $M \equiv N \pmod{AA'}$ setzt die Theilbarkeit von $M - N$ durch AA' voraus, worin die Voraussetzung der Theilbarkeit durch A enthalten ist; die Theilbarkeit von $M - N$ durch A wird aber durch die Congruenz $M \equiv N \pmod{A}$ ausgedrückt.]

13. *Lehrsatz. Befriedigt $x = a$ eine Congruenz*

$$f(x) \equiv 0 \pmod{p},$$

*so befriedigen dieselbe auch alle Zahlen, welche congruent sind a nach dem Modul p**).

Beweis. Nach den im vorigen Paragraphen bemerkten Eigenschaften der Congruenzen (s. daselbst Nr. 6), folgt aus

$$X \equiv a \pmod{p}$$

die Congruenz

$$f(X) \equiv f(a) \pmod{p}.$$

Nach der Voraussetzung befriedigt aber a die Congruenz $f(x) \equiv 0 \pmod{p}$, folglich ist

$$f(a) \equiv 0 \pmod{p}$$

und nach Nr. 1 des vorigen Paragraphen folgt in unserem Falle aus $f(X) \equiv f(a) \pmod{p}$ auch die Congruenz

$$f(X) = 0 \pmod{p},$$

was zu beweisen war.

---

§ 11. **Ueber die kleinsten Reste.**

Wir haben soeben gesehen, dass wenn der Congruenz

$$f(x) \equiv 0 \pmod{p}$$

eine Zahl a genügt, derselben Congruenz auch alle Zahlen genügen müssen, welche der Zahl a nach dem Modul p congruent sind. Welche Zahlen sind es nun, die congruent sind a nach dem Modul p? Um diese Frage zu beantworten, brauchen wir nur zu bedenken, dass Zahlen unter einander nach einem Modul p congruent sind, wenn ihre Differenz durch p ohne Rest theilbar ist; so wird also X eine Zahl sein, welche congruent ist a nach dem Modul p,

*) Hier sowohl, als überhaupt in dem Folgenden, wollen wir unter den Zeichen $f(x)$, $F(x)$, $\varphi(x)$, ... ganze Functionen mit ganzen Coëfficienten verstehen.

wenn die Differenz zwischen X und a durch p theilbar ist. Bezeichnet man den Quotienten der Division von $a - X$ durch p mit N, so erhalten wir

$$\frac{a - X}{p} = N,$$

woraus für X folgt:

$$X = a - pN.$$

Dieses ist die allgemeine Formel für alle Zahlen X, welche einer Zahl a nach dem Modul p congruent sind. Ertheilt man nun hierin der Zahl N verschiedene Werthe, sowohl positive, als negative, so erhält man eine unendliche Menge von Zahlen, welche alle congruent sind a nach dem Modul p.

Unter allen Zahlen, welche einer Zahl a nach dem Modul p congruent sind, verdienen zwei eine besondere Aufmerksamkeit:

1) diejenige positive Zahl, welche unter allen nach dem Modul p der Zahl a congruenten Zahlen die kleinste ist; dieselbe ist bekannt unter dem Namen des

„*kleinsten positiven Restes der Zahl a nach dem Modul p*“;

2) diejenige negative Zahl, welche unter allen negativen, der Zahl a nach dem Modul p congruenten Zahlen den kleinsten Zahlenwerth hat; diese ist unter dem Namen des

„*kleinsten negativen Restes der Zahl a nach dem Modul p*“

bekannt.

Ausserdem werden wir noch unter den beiden genannten kleinsten Resten, dem positiven und dem negativen, denjenigen, welcher den allerkleinsten Zahlenwerth besitzt, mit einer besonderen Benennung des

„*absolut kleinsten Restes der Zahl a nach dem Modul p*“

auszeichnen. In dem besonderen Falle, wenn die absoluten Werthe beider kleinsten Reste — des kleinsten positiven und des kleinsten negativen Restes — der Zahl a nach dem Modul p einander gleich sind, können wir ohne

Unterschied den *einen* oder den *anderen* der kleinsten Reste als *absolut kleinsten* wählen und wir sagen dann:

> „*der absolut kleinste Rest der Zahl a nach dem Modul p hat in diesem Falle zwei Werthe.*"

Nach der Formel

$$X = a - Np,$$

welche alle Zahlen überhaupt, die der Zahl a nach dem Modul p congruent sind, definirt, ist es leicht, sowohl den kleinsten positiven Rest der Zahl a nach dem Modul p, als auch den kleinsten negativen Rest derselben zu finden. Zu diesem Zwecke schreiben wir die Gleichung $X = a - Np$ in der Form

$$X = p\left(\frac{a}{p} - N\right);$$

woraus ersichtlich wird, dass der kleinste Zahlenwerth von X denjenigen Werthen von N entspricht, welche sich dem Bruche $\frac{a}{p}$ am meisten nähern; zugleich ist aber auch ersichtlich, dass X einen positiven, oder negativen Werth besitzt, je nachdem N [algebraisch*)] kleiner, oder grösser als $\frac{a}{p}$ ist.

Folglich wird der kleinste positive Rest einer Zahl a nach dem Modul p dadurch erhalten, dass man in $a - Np$ für N eine Zahl nimmt, welche $\frac{a}{p}$ am nächsten und nicht grösser als $\frac{a}{p}$ ist. Eine solche Zahl N erhalten wir offenbar, wenn a positiv ist, in dem Quotienten der Division von a durch p, indem wir den Rest vernachlässigen; N ist dann positiv; [und, wenn a negativ ist, in dem um Eins vermehrten absoluten Werth des genannten Quotienten, welche Summe dann für N negativ genommen wird].

Daraus ist also klar, dass wir *den kleinsten positiven Rest nach dem Modul p einer positiven Zahl a in dem*

[*) Nach Cauchy soll n *algebraisch-kleiner* als m heissen, wenn man zu n eine *positive* Zahl addiren muss, um m zu erhalten.]

Quotienten der Division derselben durch p finden [*und einer* n e g a t i v e n *Zahl a in dem um Eins vermehrten absoluten Werth des genannten Quotienten, welcher dann negativ genommen wird*].

[Ist a dem absoluten Werthe nach kleiner als p, so wird der Quotient der Division von a durch p Null und es ist dann für N bei positivem a der Werth $N = 0$ und bei negativem a der Werth $N = -1$ zu nehmen].

So werden wir z. B. zur Bestimmung des kleinsten positiven Restes von 23 nach dem Modul 7, in der Formel $X = 23 - 7N$ für N diejenige ganze Zahl nehmen, welche durch Division von 23 durch 7 erhalten wird. Indem wir die Division ausführen, finden wir in unserem Falle $N = 3$. Setzen wir $N = 3$ in unsere Formel $23 - 7N$ ein, so finden wir 2 als kleinsten positiven Rest von 23 nach dem Modul 7.

Ebenso finden wir den kleinsten positiven Rest von (-2) nach dem Modul 5 nach der Formel $-2-5N$, wobei für N genommen werden muss die $\frac{-2}{5}$ am nächsten liegende ganze Zahl, welche jedoch $\frac{-2}{5}$ [algebraisch] nicht übertrifft. Eine solche Zahl ist (-1); folglich ist der gesuchte positive Rest $-2+5 = 3$.

Es ist nicht schwer, sich zu überzeugen, dass der kleinste positive Rest von a nach dem Modul p *immer* kleiner als p sein muss. Dieses folgt aus dem, was wir über die Bestimmung dieses Restes ausgesagt haben. Wir haben nämlich gesehen, dass derselbe durch die Formel $a-Np$ bestimmt wird, wobei N eine ganze Zahl ist, welche $\frac{a}{p}$ am nächsten kommt; folglich ist $\frac{a}{p} - N < 1$ und somit

$$a - Np = p\left(\frac{a}{p} - N\right) < p.$$

Um den kleinsten negativen Rest einer Zahl a nach dem Modul p zu bestimmen, müssen wir in der Formel $a - Np$, oder $p\left(\frac{a}{p} - N\right)$ für N eine ganze Zahl nehmen,

welche [im algebraischen Sinne] grösser als $\frac{a}{p}$ wäre und $\frac{a}{p}$ am nächsten käme. Eine solche Zahl ist für ein positives a offenbar diejenige, welche dadurch erhalten wird, dass man bei der Division von a durch p in dem Quotienten der Division den noch übrig bleibenden echten Bruch durch Eins ersetzt. [Bei einem negativen a nehme man für N direct den ganzzahligen Quotienten. Der kleinste postive Rest einer positiven Zahl und der kleinste negative Rest einer negativen Zahl werden also gleichartig bestimmt und der kleinste positive Rest einer negativen Zahl wie der kleinste negative Rest einer positiven Zahl.] So wird der kleinste negative Rest von 23 nach dem Modul 7 durch die Formel $23 - 7N$ bestimmt, wobei für N, anstatt $\frac{23}{7} = 3 + \frac{2}{7}$, genommen wird $3 + 1$, indem der Bruch $\frac{2}{7}$ durch Eins ersetzt wird. Setzt man $N = 4$ in $23 - 7N$, so findet man $23 - 7.4 = (-5)$ als den kleinsten negativen Rest von 23 nach dem Modul 7. [In gleicher Weise findet man den kleinsten negativen Rest von (-2) nach dem Modul 5, indem man in $-2 + 5N$ für N den ganzzahligen Quotienten Null setzt, welcher bei der Division $\frac{-2}{5}$ herauskommt.]

Hat man für eine Zahl nach einem gegebenem Modul den kleinsten *positiven* und den kleinsten *negativen* Rest bestimmt, so erkennt man dann leicht, welcher von ihnen als der *absolut* kleinste Rest zu betrachten ist. Allein man kann den absolut kleinsten Rest auch *direct* aus der Formel $a - Np$, oder $p\left(\frac{a}{p} - N\right)$ bestimmen. Man braucht zu diesem Zwecke nur N so zu wählen, dass $\frac{a}{p} - N$ den *kleinsten Zahlenwerth* erhalte. Einen solchen Werth für N erhalten wir offenbar dadurch, dass wir den Quotienten der Division von a durch p bilden und den dabei auftretenden Bruch vernachlässigen, wenn derselbe kleiner als $\frac{1}{2}$, oder denselben durch Eins ersetzen, wenn er grösser

als $\frac{1}{2}$ ist. Ist der betreffende echte Bruch weder grösser noch kleiner als $\frac{1}{2}$, so können wir denselben nach Willkür entweder vernachlässigen, oder durch Eins ersetzen; in dem einen, wie in dem anderen Falle wird der absolute Werth der Grösse $\frac{a}{p} - N$ gleich sein $\frac{1}{2}$.

So hat man z. B. bei der Bestimmung des absolut kleinsten Restes von 23 nach dem Modul 7 in $23 - 7N$ für N den Quotienten $\frac{23}{7} = 3 + \frac{2}{7}$ zu nehmen, indem man den Bruch $\frac{2}{7} < \frac{1}{2}$ vernachlässigt. Dieses giebt $N = 3$ und somit ist der gesuchte absolut kleinste Rest:

$$23 - 7 \,.\, 3 = 2.$$

Dagegen hat man bei der Bestimmung des absolut kleinsten Restes von 25 nach dem Modul 7 für N in $25 - 7N$ den Quotienten $\frac{25}{7} = 3 + \frac{4}{7}$ zu bilden und den Bruch $\frac{4}{7} > \frac{1}{2}$ durch Eins zu ersetzen. Dieses giebt $N = 4$ und somit wird der gesuchte absolut kleinste Rest

$$25 - 7 \,.\, 4 = -3.$$

Aus dem Gesagten geht hervor, dass wir bei der Bestimmung des absolut kleinsten Restes in der Formel $a - Np$ für N eine ganze Zahl zu nehmen haben, welche mit $\frac{a}{p}$ eine Differenz liefert, die im absoluten Werthe nicht grösser als $\frac{1}{2}$ wird. Und somit *hat der absolut kleinste Rest einer Zahl a nach dem Modul p, indem derselbe durch die Formel $a - Np$, oder $p\left(\frac{a}{p} - N\right)$ bestimmt wird, einen absoluten Werth, welcher nicht grösser ist als* $\frac{p}{2}$.

---

§ 12. Ueber die Anzahl der Lösungen einer Congruenz.

Nachdem wir die Zahlen untersucht haben, welche congruent sind a nach dem Modul p, wollen wir uns der Lösung der Congruenz $f(x) \equiv 0 \pmod{p}$ zuwenden.

Wir haben bereits gesehen, dass wenn dieser Congruenz eine gewisse Zahl a genügt, derselben auch jede Zahl X genügt, für welche die Congruenz $X \equiv a \pmod{p}$ stattfindet. Solcher Zahlen giebt es unendlich viele; aber alle diese Zahlen, indem sie alle einer und derselben Zahl a und folglich auch unter einander congruent sind nach dem Modul p, werden als *eine* Lösung der Congruenz $f(x) \equiv 0 \pmod{p}$ angesehen. Genügen daher einer Congruenz

$$f(x) \equiv 0 \pmod{p}$$

nur solche Zahlen x, für welche die Congruenz

$$x \equiv a \pmod{p}$$

besteht, so sagen wir: „*die Congruenz* $f(x) \equiv 0 \pmod{p}$ *lässt nur eine Lösung zu.*“ Dagegen werden wir sagen: „*die Congruenz* $f(x) \equiv 0 \pmod{p}$ *habe zwei Lösungen*“, wenn derselben ausser den Zahlen, welche durch die Congruenz

$$x \equiv a \pmod{p}$$

definirt sind, auch diejenigen genügen, welche aus einer Congruenz

$$x \equiv a_1 \pmod{p}$$

erhalten werden, wobei unter a und a_1 eine Congruenz

$$a \equiv a_1 \pmod{p}$$

nicht besteht. Und ebenso werden wir allgemein sagen:

eine Congruenz

$$f(x) \equiv 0 \pmod{p}$$

besitze n Lösungen, wenn derselben solche und nur solche Zahlen genügen, welche durch die Congruenzen

$$\left.\begin{array}{l} x \equiv a \\ x \equiv a_1 \\ x \equiv a_2 \\ \quad\vdots \\ x \equiv a_{n-1} \end{array}\right\} \pmod{p}$$

definirt sind, wobei $a, a_1, a_2, \ldots . a_{n-1}$ *solche Zah-*

len bedeuten, welche unter einander nicht congruent sind nach dem Modul p,

Auf Grund dieser Definition beweisen wir folgenden

14. *Lehrsatz. Eine Congruenz*

$$f(x) \equiv 0 \pmod{p}$$

hat so viele Lösungen, wie viele Zahlen aus der Reihe

$$0, 1, 2, \ldots, p-1$$

dieselbe befriedigen und, sind

$$\alpha_1, \alpha_2, \alpha_3, \ldots \alpha_n$$

solche Zahlen, so sind

$$x \equiv \alpha_1;\ x \equiv \alpha_2;\ x \equiv \alpha_3;\ \ldots;\ x \equiv \alpha_n \pmod{p}$$

die Lösungen der Congruenz

$$f(x) \equiv 0 \pmod{p}.$$

Beweis. In § 10 haben wir gesehen, dass wenn

$$\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n$$

der Congruenz $f(x) \equiv 0 \pmod{p}$ genügen, derselben auch alle Zahlen genügen, welche durch die Congruenzen

$$x \equiv \alpha_1;\ x \equiv \alpha_2;\ x \equiv \alpha_3;\ \ldots;\ x \equiv \alpha_n \pmod{p}$$

definirt sind. Es ist aber nicht schwer zu beweisen, dass es, *einerseits*, ausser diesen Zahlen keine mehr geben kann, welche der Congruenz $f(x) \equiv 0 \pmod{p}$ genügen sollte, und dass, *andererseits*, die Zahlen $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n$ untereinander nach dem Modul p *incongruent* sind, woraus, nach dem oben über die Anzahl der Lösungen einer Congruenz $f(x) \equiv 0 \pmod{p}$ Ausgesagten, die Richtigkeit des oben ausgesprochenen Lehrsatzes folgen würde.

Um nun *Ersteres* zu beweisen, wollen wir das Gegentheil annehmen, es befriedige nämlich die Congruenz $f(x) \equiv 0 \pmod{p}$ irgend eine Zahl A, welche keine einzige der Congruenzen

$$x \equiv \alpha_1;\ x \equiv \alpha_2;\ x \equiv \alpha_3;\ \ldots;\ x \equiv \alpha_n \pmod{p}$$

befriedigt.

Befriedigt A die Congruenz $f(x) \equiv 0 \pmod{p}$, so thut es (nach § 10) auch jede Zahl, welche congruent ist A nach dem Modul p, folglich auch der kleinste positive Rest von A nach dem Modul p. Bezeichnen wir diesen Rest mit α, so erhalten wir

$$\left.\begin{array}{r} A \equiv \alpha \\ f(\alpha) \equiv 0 \end{array}\right\} \pmod{p}, \quad . \quad . \quad . \quad . \quad . \quad . \quad (4)$$

wobei α, als kleinster positiver Rest von A nach dem Modul p, unter den Zahlen der Reihe

$$0,\ 1,\ 2,\ \ldots.,\ p-1$$

enthalten sein muss. Ist aber α in dieser Reihe enthalten und befriedigt es $f(x) \equiv 0 \pmod{p}$, so muss α eine der Zahlen $\alpha_1, \alpha_2, \alpha_3, \ldots., \alpha_n$ sein; weil nach der Voraussetzung $\alpha_1, \alpha_2, \alpha_3, \ldots., \alpha_n$ die einzigen Zahlen der Reihe $0, 1, 2, \ldots., p-1$ sind, welche $f(x) \equiv 0 \pmod{p}$ befriedigen. Dieses ist aber unmöglich: weil A, nach (4), die Congruenz $x \equiv \alpha$ befriedigt, während nach der Voraussetzung A keiner der Congruenzen

$$x \equiv \alpha_1;\ x \equiv \alpha_2;\ \ldots.;\ x \equiv \alpha_n \pmod{p}$$

genügen soll.

Wenden wir uns nun zu dem Beweise, dass die Zahlen $\alpha_1, \alpha_2, \ldots., \alpha_n$ nicht unter einander congruent sind nach dem Modul p.

Lassen wir das Gegentheil zu und mag etwa

$$\alpha_1 \equiv \alpha_2 \pmod{p}$$

sein. Aus dieser Congruenz folgt aber die Theilbarkeit von $\alpha_1 - \alpha_2$ durch p, welche unmöglich ist; weil α_1 und α_2 positive Zahlen sind, von denen jede kleiner ist als p, infolge dessen der absolute Werth der Differenz $\alpha_1 - \alpha_2$ jedenfalls kleiner als p sein muss und somit nicht durch p theilbar sein kann.

So überzeugen wir uns von der Richtigkeit des ausgesprochenen Lehrsatzes.

Um eine Anwendung dieses Lehrsatzes sofort zu zeigen, nehmen wir an: $f(x) = x^3 - x - 1$ und $p = 5$, also

$$x^3 - x - 1 \equiv 0 \pmod{5}.$$

Indem wir hierin anstatt x die Werthe

$$0,\ 1,\ 2,\ 3,\ 4$$

einsetzen, überzeugen wir uns, dass nur die Zahl 2 der betrachteten Congruenz genügt; woraus wir schliessen, dass unsere Congruenz *eine* Lösung

$$x \equiv 2 \pmod{5}$$

besitzt.

In derselben Weise überzeugen wir uns, dass die Congruenz

$$x^2 - 3 \equiv 0 \pmod{11}$$

zwei Lösungen

$$\left.\begin{array}{l} x \equiv 5 \\ x \equiv 6 \end{array}\right\} \pmod{11}$$

besitzt.

Indem wir dagegen die Congruenz

$$x^2 - 11 \equiv 0 \pmod{3}$$

ebenso behandeln, überzeugen wir uns, dass dieselbe durch keine der Zahlen

$$0,\ 1,\ 2$$

befriedigt wird; diese Congruenz hat also nach unserer Definition gar keine Lösung.

Kapitel II.

Ueber die Congruenz ersten Grades.

---

§ 13. Lösung der Congruenzen ersten Grades, wenn der Modul relativ prim ist zu dem Coëfficienten der Unbekannten.

Die allgemeine Gestalt einer Congruenz ersten Grades ist

$$ax - b \equiv 0 \pmod{p},$$

wobei a, b irgend welche positive, oder negative ganze Zahlen, während p eine positive ganze Zahl bedeuten soll. Congruenzen dieser Gestalt bieten zwei wesentlich von einander verschiedene Fälle dar, welche wir gesondert der Betrachtung unterziehen wollen. Der erste Fall sei der, wenn a und p relativ prim zu einander sind; der zweite, — wenn dieselben einen gemeinschaftlichen Theiler besitzen. Wir beginnen mit dem ersten Falle und beweisen folgenden

15. *Lehrsatz. Die Congruenz*

$$ax - b \equiv 0 \pmod{p}$$

hat, wenn a und p relativ prim zu einander sind, immer eine und nur eine Lösung.

Beweis. Aus dem, was wir in § 12 über die Anzahl der Lösungen einer Congruenz $f(x) \equiv 0 \pmod{p}$ überhaupt bewiesen haben, folgt, dass unsere Congruenz $ax - b \equiv 0 \pmod{p}$ genau so viele Lösungen hat, als es unter den Zahlen der Reihe

$$0, 1, 2, \ldots, p-1$$

solche giebt, welche die Congruenz $ax-b \equiv 0 \pmod{p}$ befriedigen, oder, was nach der Definition ein und dasselbe ist, wie viele es in der Reihe

$$a.0-b;\ a.1-b;\ a.2-b;\ \ldots;\ a(p-1)-b$$

Zahlen giebt, welche durch p theilbar sind. Da aber diese ganze Zahlenreihe überhaupt eine arithmetische Progression bildet, deren Differenz die Zahl a ist, welche nach der Voraussetzung relativ prim zu p war, während die Anzahl aller Glieder der Reihe p beträgt, so wird hier (nach dem 10ten Lehrsatz) *ein* und *nur ein* Glied vorhanden sein, welches durch p theilbar ist. Folglich hat die Congruenz $ax-b \equiv 0 \pmod{p}$, bei der gemachten Voraussetzung immer eine und nur eine Lösung, was wir beweisen wollten.

Nachdem wir uns auf diese Weise überzeugt haben, dass in dem betrachteten Falle die Congruenz $ax-b \equiv 0 \pmod{p}$ immer eine Lösung besitzt, wollen wir nunmehr zeigen, wie man diese Lösung wirklich finden kann. Man besitzt heut zu Tage in der Wissenschaft mehrere Methoden, um die Congruenz $ax-b \equiv 0 \pmod{p}$ zu lösen. Die bemerkenswürdigsten unter denselben wollen wir später, wo wir von eigenthümlichen Eigenschaften der Zahlen, auf welchen die Methoden beruhen, handeln werden, auseinandersetzen. Hier wollen wir nur bemerken, dass die Congruenz $ax-b \equiv 0 \pmod{p}$ nach derselben Methode gelöst werden kann, welche in der Algebra für die Lösung der unbestimmten Gleichung mit zwei Unbekannten

$$ax-pz = b,$$

gegeben wird, die sich von der Congruenz

$$ax-b \equiv 0 \pmod{p}$$

lediglich in der Bezeichnungsweise unterscheidet. In der That drückt die Congruenz $ax-b \equiv 0 \pmod{p}$ nichts Anderes aus als die Theilbarkeit der Differenz $ax-b$ durch p, was auch durch die Gleichung

$$\frac{ax-b}{p} = z$$

dargestellt werden kann, wenn man in z eine beliebige ganze Zahl voraussetzt. Daraus erhalten wir eben zur Bestimmung von x und z die Gleichung in ganzen Zahlen

$$ax - pz = b.$$

Durch die ganzzahlige Lösung der unbestimmten Gleichung $ax - pz = b$ wird also der Werth von x bestimmt, welcher die Congruenz $ax - b \equiv 0 \pmod{p}$ befriedigt. Diese Werthe von x werden, wie wir wissen, in der Form $x = \alpha + np$ dargestellt, wobei α einer solcher Werthe von x ist, welche die Fähigkeit haben, die Gleichung $ax - pz = b$ zu befriedigen, und wobei n eine beliebige ganze Zahl ist. Nach der eingeführten Bezeichnung werden wir, anstatt

$$x = \alpha + np,$$

wobei n als beliebige ganze Zahl vorausgesetzt wird, die Schreibweise gebrauchen:

$$x \equiv \alpha \pmod{p}$$

und in dieser Gestalt werden wir immer die Lösung der Congruenz $ax - b \equiv 0 \pmod{p}$ darstellen.

Hat man z. B. die Congruenz

$$7x - 3 \equiv 0 \pmod{10}$$

zu lösen, so nehme man die Gleichung

$$7x - 10z = 3.$$

Löst man diese Gleichung nach der in der elementaren Algebra angegebenen Methode, so erhält man für x und z die Ausdrücke:

$$x = 9 + 10n,$$
$$z = 6 + 7n,$$

woraus wir als Lösung unserer Congruenz

$$7x - 3 \equiv 0 \pmod{10}$$

erhalten:

$$x \equiv 9 \pmod{10}.$$

§ 14. **Die Lehrsätze von Fermat und Euler.**

Auf Grund der oben in Bezug auf Congruenzen überhaupt, wie auf die specielle Congruenz $ax - b \equiv 0 \pmod{p}$ insbesondere bewiesenen Lehrsätze, sind wir nunmehr im Stande, über gewisse Eigenschaften ganzer Zahlen zwei sehr merkwürdige Lehrsätze zu beweisen, welche für die Zahlentheorie überhaupt sehr wichtig sind und welche zugleich auch eine Lösung der Congruenz ersten Grades liefern werden. Mit diesen Eigenschaften der Zahlen wollen wir uns eben beschäftigen.

16. *Lehrsatz. Ist p eine Primzahl und kein Divisor von a, so ist*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Beweis. Mögen

$$r_1, r_2, r_3, \ldots., r_{p-1}$$

die jeweiligen kleinsten positiven Reste der Zahlen

$$1a, 2a, 3a, \ldots., (p-1)a$$

nach dem Modul p bedeuten, so werden dieselben die Congruenzen

$$(5) \quad \ldots\ldots \quad \left.\begin{array}{r} 1a \equiv r_1 \\ 2a \equiv r_2 \\ 3a \equiv r_3 \\ \vdots \\ (p-1)\,a \equiv r_{p-1} \end{array}\right\} \pmod{p}$$

befriedigen. Multipliciren wir alle diese Congruenzen gliedweise mit einander, so erhalten wir

$$(6) \quad 1 \,.\, 2 \,.\, 3 \ldots. (p-1)\, a^{p-1} \equiv r_1\, r_2\, r_3 \ldots. r_{p-1} \pmod{p}.$$

Es ist aber nicht schwer sich zu überzeugen, dass die Producte

$$1 \,.\, 2 \,.\, 3 \ldots. (p-1),$$
$$r_1\, r_2\, r_3 \ldots. r_{p-1}$$

einander gleich sind.

Zu diesem Ende bemerken wir, dass

$$r_1, r_2, r_3, \ldots., r_{p-1},$$

als kleinste positiven Reste der Zahlen

$$1a,\ 2a,\ 3a,\ \ldots.,\ (p-1)a$$

nach dem Modul p, überhaupt keine anderen Werthe, wie

$$0,\ 1,\ 2,\ \ldots.,\ p-1,$$

haben können.

Dabei kann aber kein einziger dieser Reste den Werth Null haben; denn würden wir das Gegentheil zulassen, so würde die Congrnenz (6) die Theilbarkeit von

$$1\,.\,2\,.\,3\ \ldots.\ (p-1)\,a^{p-1}$$

durch p behaupten, während $1, 2, 3, \ldots., p-1$ und a alle relativ prim zu p sind. Folglich können die Zahlen

$$r_1,\ r_2,\ r_3,\ \ldots.,\ r_{p-1}$$

keine anderen Werthe haben als solche, welche in

$$1,\ 2,\ 3,\ \ldots.,\ p-1$$

enthalten sind.

Unter den Zahlen $r_1, r_2, r_3, \ldots., r_{p-1}$ können aber nicht zwei einander gleich sein. Denn, würden wir zulassen, es sei etwa

$$r_m = r_\mu = b,$$

so würde nach (5) folgen:

$$\left.\begin{array}{l} ma \equiv b \\ \mu a \equiv b \end{array}\right\} \pmod{p},$$

wobei m und μ zwei Zahlen sind aus der Reihe

$$1,\ 2,\ 3,\ \ldots.,\ p-1,$$

und wir hätten somit für die Congruenz

$$ax \equiv b \pmod{p}$$

zwei Lösungen:

$$x \equiv m \pmod{p} \text{ und } x \equiv \mu \pmod{p},$$

was (nach Lehrsatz 15) unmöglich ist.

Daraus folgt, dass unter den Elementen der Reihe

$$r_1,\ r_2,\ r_3,\ \ldots.,\ r_{p-1}$$

nur die Zahlen

$$1,\ 2,\ 3,\ \ldots.,\ p-1$$

sich vorfinden können und zwar jede nur einmal. Da aber die Reihen

$$r_1, r_2, r_3, \ldots, r_{p-1};$$
$$1, 2, 3, \ldots, p-1$$

eine gleiche Anzahl von Gliedern besitzen, so müssen in der ersteren auch *alle* Glieder der zweiten wirklich vorhanden sein. Somit bestehen beide Reihen aus ein und denselben Zahlen und in jeder Reihe kommt jede Zahl nur einmal vor und somit muss das Product aller Glieder der ersten Reihe dem Producte aller Glieder der zweiten gleich sein. Haben wir uns davon überzeugt, so können wir in (6) das Product $r_1 . r_2 . r_3 \ldots . r_{p-1}$ durch das Product $1 . 2 . 3 \ldots . p-1$ ersetzen und erhalten auf diese Weise

$$1 . 2 . 3 \ldots . (p-1) a^{p-1} \equiv 1 . 2 . 3 \ldots . (p-1) \pmod{p}.$$

Man darf aber beide Seiten dieser Congruenz durch die Zahlen 2, 3, ... $(p-1)$ dividiren; weil nämlich alle diese Zahlen, indem sie kleiner als p sind, zu der Primzahl p relativ prim sein müssen. Führen wir diese Division aus, so erhalten wir

$$a^{p-1} \equiv 1 \pmod{p},$$

w. z. b. w.

So erhalten wir z. B. für $p = 7$ und $a = 2$ die Congruenz

$$2^{7-1} \equiv 1 \pmod{7},$$

von deren Richtigkeit wir uns sofort überzeugen, indem wir bemerken, dass $2^6 = 64$ und $64 \equiv 1 \pmod{7}$ ist.

Dieser Lehrsatz ist einer der bemerkenswerthesten in der Zahlentheorie und lässt sehr wichtige Anwendungen zu. Derselbe ist zuerst von Fermat entdeckt, war aber von Fermat ohne Beweis ausgesprochen. Der erste, dem es gelungen ist, diesen „*Fermat'schen Satz*“ zu beweisen, war Euler; Letzterer gab auch zugleich folgenden allgemeineren Lehrsatz.

17. Lehrsatz. *Bedeutet n die Anzahl aller Zahlen, welche kleiner als N und relativ prim*

zu N sind und ist a relativ prim zu N, so ist immer

$$a^n \equiv 1 \pmod{N}.$$

Beweis. Bezeichnet man mit

$$N_1, N_2, N_3, \ldots, N_n$$

die Zahlen, welche relativ prim zu N und kleiner als N sind, und mit

$$r_1, r_2, r_3, \ldots, r_n,$$

die in Bezug auf den Modul N kleinsten positiven Reste der Zahlen

$$aN_1, aN_2, aN_3, \ldots, aN_n,$$

so erhält man das System von Congruenzen:

$$\left.\begin{array}{c} aN_1 \equiv r_1 \\ aN_2 \equiv r_2 \\ \vdots \\ aN_n \equiv r_n \end{array}\right\} \pmod{N}, \quad \ldots\ldots \quad (7)$$

welches durch gliedweise Multiplication die Congruenz

$$N_1 N_2 \ldots N_n a^n \equiv r_1 r_2 \ldots r_n \pmod{N}, \quad \ldots \quad (8)$$

liefert.

Es ist aber leicht sich zu überzeugen, dass die Producte

$$N_1 N_2 \ldots N_n \text{ und } r_1 r_2 \ldots r_n$$

einander gleich sind.

Da nämlich $r_1, r_2, \ldots, r_n$ die nach dem Modul N kleinsten positiven Reste von $aN_1, aN_2, \ldots, aN_n$ bedeuten, so können dieselben keine anderen Werthe als

$$0, 1, 2, \ldots, N-1$$

haben; aber auch unter diesen Werthen sind für $r_1, r_2, \ldots r_n$ nur diejenigen möglich, welche keinen gemeinschaftlichen Theiler mit N haben; weil die Congruenz (8), deren linke Seite aus einem Producte von lauter solchen Zahlen besteht, die relativ prim zu N sind, [nach Eigensch. 8 in § 9] voraussetzt, dass auch $r_1, r_2, \ldots, r_n$ und N keinen gemeinschaftlichen Theiler besitzen.

Daraus folgt, dass für

$$r_1, r_2, \ldots, r_n$$

nur die Werthe

$$N_1, N_2, \ldots, N_n$$

möglich sind.

Es ist aber klar, dass nicht irgend zwei der Zahlen

$$r_1, r_2, \ldots, r_n$$

einander gleich sein können; denn im Falle der Gleichheit zweier derselben, wie etwa

$$r_m = r_\mu = b,$$

würden wir nach (7) die Congruenzen

$$\left. \begin{array}{l} aN_m \equiv b \\ aN_\mu \equiv b \end{array} \right\} \pmod{N}$$

erhalten, wobei m und μ irgend welche zwei Zahlen aus der Reihe $1, 2, 3, \ldots, N-1$ bedeuten und somit würden wir für die Congruenz ersten Grades

$$ax \equiv b \pmod{N}$$

zwei Lösungen gefunden haben, was [nach Lehrsatz 15] nicht möglich ist.

Hieraus folgt, dass unter den Gliedern der Reihe

$$r_1, r_2, \ldots, r_n$$

sich nur die Zahlen

$$N_1, N_2, \ldots, N_n$$

vorfinden können, und zwar jede derselben nur ein einziges Mal. Da aber beide Reihen eine gleiche Anzahl Glieder haben, so müssen in der ersten Reihe auch *alle* Zahlen der zweiten vertreten sein; so dass beide Reihen aus ein und denselben Zahlen zusammengesetzt sind und in jeder dieser Reihen tritt jede Zahl nur einmal auf. Das Product aller Zahlen der ersten Reihe muss also dem Producte aller Zahlen der zweiten gleich sein; und wir können somit in (8) das Product $r_1 r_2 r_3 \ldots r_n$ durch das Product $N_1 N_2 N_3 \ldots N_n$ ersetzen und somit

$$N_1 N_2 \ldots N_n a^n \equiv N_1 N_2 \ldots N_n \pmod{N}$$

erhalten. Es sind aber N_1, N_2, ..., N_n und folglich ist auch das Product derselben relativ prim zum Modul N und man darf sonach beide Seiten der Congruenz durch das Product $N_1 N_2 \dots N_n$ dividiren. Indem wir diese Division ausführen, erhalten wir aber die Congruenz

$$a^n \equiv 1 \pmod{N},$$

wie in dem verallgemeinerten Fermat'schen Lehrsatze von Euler behauptet wurde.

Ist z. B. $N = 20$ und $a = 3$, so erhält man aus Lehrsatz 12 für die Grösse n, welche angiebt, wie viel Zahlen kleiner als 20 und relativ prim zu 20 sind, weil $20 = 2^2.5$ ist, die Formel

$$n = 20\,(1-\tfrac{1}{2})\,(1-\tfrac{1}{5}) = 20\left(\frac{2-1}{2}\right)\left(\frac{5-1}{5}\right) = 8$$

und nach dem Euler'schen Satze wird also

$$3^8 \equiv 1 \pmod{20},$$

sein müssen. Von der Richtigkeit dieser Behauptung überzeugen wir uns sofort, indem wir finden:

$$3^8 = 6561 \text{ und } 6561 \equiv 1 \pmod{20}.$$

---

§ 15. Anwendung der Sätze von Fermat und Euler auf die Lösung der Congruenz ersten Grades.

Auf Grund der eben bewiesenen Lehrsätze von Fermat und Euler kann man nun eine einfache Lösung der Congruenz

$$ax - b \equiv 0 \pmod{p}$$

finden, wenn man, wie früher, voraussetzt, dass a relativ prim zu p sei.

Wir wollen mit dem einfacheren Falle beginnen, wenn nämlich p eine Primzahl ist.

Da a relativ prim zu p vorausgesetzt war, so ist, wenn p eine Primzahl ist, (nach § 3) nothwendig [und hinreichend], dass a durch p nicht theilbar sei. Nach

dem Fermat'schen Satze (so werden wir in der Folge immer den Lehrsatz 16 nennen) wird nun die Congruenz stattfinden

$$a^{p-1} \equiv 1 \pmod{p},$$

welche durch Multiplication beider Seiten mit b und Subtraction von b, so geschrieben werden kann:

$$a \,.\, b\,a^{p-2} - b \equiv 0 \pmod{p}.$$

Vergleicht man diese Congruenz mit der, welche wir zu lösen haben, nämlich:

$$ax - b \equiv 0 \pmod{p},$$

so bemerken wir, dass letztere befriedigt werden muss, wenn man für x setzt: $x = b\,a^{p-2}$; folglich ist die vollständige Lösung derselben

$$x \equiv b a^{p-2} \pmod{p}.$$

In dieser Weise bestimmt sich also die Lösung der Congruenz ersten Grades

$$ax - b \equiv 0 \pmod{p},$$

wenn p eine Primzahl und kein Divisor ist von a.

So finden wir z. B. für die Congruenz

$$3x - 8 \equiv 0 \pmod{5}$$

die Lösung

$$x \equiv 8 \,.\, 3^{5-2} \pmod{5},$$

oder, was dasselbe ist,

$$x \equiv 216 \pmod{5}.$$

Diese Lösung der Congruenz kann man noch auf eine einfachere Form zurückführen, indem man 216 durch den kleinsten positiven Rest von 216 nach dem Modul 5 ersetzt. Man findet auf diese Weise

$$x \equiv 1 \pmod{5}$$

als Lösung der Congruenz

$$3x - 8 \equiv 0 \pmod{5}.$$

Gehen wir nun zu der Lösung solcher Congruenzen über, deren Modul eine zusammengesetzte Zahl ist.

Es mag die Congruenz

$$ax - b \equiv 0 \pmod{N}$$

gegeben sein, wobei N eine beliebige ganze positive Zahl ist, während a, wie früher vorausgesetzt worden, relativ prim zu N ist.

Nach dem Euler'schen Satze (Lehrsatz 17) erhalten wir

$$a^n \equiv 1 \pmod{N},$$

wenn wir mit n die Anzahl der Zahlen bezeichnen, welche relativ prim zu N und kleiner als N sind. Durch Multiplication beider Seiten mit b und Subtraction von b können wir diese Congruenz so schreiben:

$$a \,.\, b a^{n-1} - b \equiv 0 \pmod{N}.$$

Vergleichen wir diese letztere mit der gegebenen Congruenz

$$ax - b \equiv 0 \pmod{N},$$

so finden wir die Lösung derselben in der Form

$$x \equiv b a^{n-1} \pmod{N}.$$

Was nun die Bedeutung von n betrifft, welche die Anzahl der Zahlen angeben soll, die relativ prim zu N und kleiner als N sind, so können wir dieselbe nach Lehrsatz 12 leicht finden. Es ist nämlich

$$n = \alpha^m \beta^{m'} \gamma^{m''} \ldots . \left(\frac{\alpha-1}{\alpha}\right) \left(\frac{\beta-1}{\beta}\right) \left(\frac{\gamma-1}{\gamma}\right) \ldots .,$$

wenn N bei Zerlegung in Primfactoren auf die Form

$$N = \alpha^m \beta^{m'} \gamma^{m''} \ldots .$$

gebracht wird, wobei $\alpha, \beta, \gamma, \ldots .$ von einander verschiedene Primzahlen bedeuten.

Auf diese Weise überzeugen wir uns also, dass die Lösung der allgemeinen Congruenz ersten Grades

$$ax - b \equiv 0 \pmod{\alpha^m \beta^{m'} \gamma^{m''} \ldots .},$$

wobei $\alpha, \beta, \gamma, \ldots .$ von einander verschiedene Primzahlen sind [und a keine dieser Primzahlen als Factor besitzt] durch die Formel

$$x \equiv b\,a^{\alpha^m \beta^{m'} \gamma^{m''} \dots \left(\frac{\alpha-1}{\alpha}\right)\left(\frac{\beta-1}{\beta}\right)\left(\frac{\gamma-1}{\gamma}\right) \dots -1} \pmod{\alpha^m \beta^{m'} \gamma^{m''} \dots}$$

gegeben ist.

So finden wir z. B. für die Lösung der Congruenz

$$2x - 7 \equiv 0 \pmod{15},$$

da $15 = 3^1 . 5^1$ ist, die Formel

$$x \equiv 7 . 2^{3.5\left(\frac{3-1}{3}\right)\left(\frac{5-1}{5}\right)-1} \pmod{15},$$

oder

$$x \equiv 896 \pmod{15}$$

und, indem wir noch 896 durch den kleinsten positiven Rest nach dem Modul 15 ersetzen, erhalten wir die Lösung in der einfacheren Gestalt:

$$x \equiv 11 \pmod{15}.$$

Hiermit schliessen wir die Untersuchung desjenigen Falles der Congruenz ersten Grades ab, bei welchem der Modul und der Coëfficient der Unbekannten relativ prim zu einander sind und wenden uns nunmehr zu dem Falle, dass diese Zahlen einen gemeinschaftlichen Factor besitzen.

---

§ 16. Ueber Congruenzen [ersten Grades], bei denen der Modul und der Coëfficient der Unbekannten einen gemeinschaftlichen Factor besitzen.

Nach der in § 10 gezeigten Eigenschaft der Congruenzen ist die Congruenz

$$ax \equiv b \pmod{p}$$

überhaupt unmöglich, wenn a und p einen gemeinschaftlichen Factor besitzen, der kein Theiler von b ist. Daraus folgt der

18. *Lehrsatz. Die Congruenz*

$$ax - b \equiv 0 \pmod{p}$$

hat keine Lösung, wenn ein gemeinschaftlicher Divisor von a und p nicht auch ein Divisor von b ist.

So überzeugen wir uns z. B. dass die Congruenzen

$$20x - 7 \equiv 0 \pmod{15},$$
$$6x - 5 \equiv 0 \pmod{9}$$

keine Lösung besitzen; [indem die erstere durch keinen der Werthe $x = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14$ und letztere durch keinen der Werthe $x = 1, 2, 3, 4, 5, 6, 7, 8$ befriedigt wird].

Es bleibt uns noch übrig den Fall zu betrachten, dass in der Congruenz

$$ax - b \equiv 0 \pmod{p}$$

die gemeinschaftlichen Theiler von a und p auch Theiler von b sind. Für eine solche Congruenz beweisen wir folgenden

19. *Lehrsatz.* *Haben a und p den grössten gemeinschaftlichen Theiler d und ist d zugleich auch ein Theiler von b, so hat die Congruenz*

$$ax - b \equiv 0 \pmod{p}$$

d Lösungen, welche so dargestellt werden können:

$$\left.\begin{aligned} x &\equiv \alpha \\ x &\equiv \alpha + \frac{p}{d} \\ x &\equiv \alpha + \frac{2p}{d} \\ &\vdots \\ x &\equiv \alpha + \frac{(d-1)p}{d} \end{aligned}\right\} \pmod{p};$$

wobei $\alpha < \frac{p}{d}$ und nicht < 0 ist und die Congruenz

$$\frac{a}{d}x - \frac{b}{d} \equiv 0 \left(\bmod.\ \frac{p}{d}\right)$$

durch α befriedigt wird.

Beweis. Ist d der grösste gemeinschaftliche Theiler von a und p und zugleich ein Theiler von b, so kann (nach § 9, Eigensch. 9) die Congruenz

$$ax - b \equiv 0 \ (\text{mod.}\ p)$$

durch Division der Glieder und des Moduls durch d auf die Form

$$\frac{a}{d}x - \frac{b}{d} \equiv 0 \left(\text{mod.}\ \frac{p}{d}\right)$$

gebracht werden, wobei

$$\frac{a}{d},\ \frac{b}{d},\ \frac{p}{d}$$

ganze Zahlen sind. Dabei sind die beiden Zahlen $\frac{a}{d}$, $\frac{p}{d}$, wie man sich leicht überzeugen kann, relativ prim zu einander, weil sonst d nicht der grösste gemeinschaftliche Theiler von a und p gewesen wäre. Wenn aber $\frac{a}{d}$, $\frac{p}{d}$ relativ prim zu einander sind, so hat ja die Congruenz

$$\frac{a}{d}x - \frac{b}{d} \equiv 0 \left(\text{mod.}\ \frac{p}{d}\right)$$

wie wir gesehen haben, immer eine Lösung, welche durch die oben angegebenen Methoden zu finden ist. Mag nun α eine Zahl sein, welche in der Reihe

$$0,\ 1,\ 2,\ \ldots,\ \frac{p}{d} - 1$$

enthalten ist, und die Congruenz

$$\frac{a}{d}x - \frac{b}{d} \equiv \left(\text{mod.}\ \frac{p}{d}\right)$$

befriedigt, so werden alle Zahlen, welche überhaupt diese Congruenz befriedigen, in

$$x \equiv \alpha \left(\text{mod.}\ \frac{p}{d}\right)$$

enthalten sein.

Dieselben Zahlen, und nur diese, befriedigen aber auch zugleich die Congruenz

$$ax - b \equiv 0 \pmod{p},$$

welche sich von

$$\frac{a}{d}x - \frac{b}{d} \equiv 0 \left(\text{mod.}\ \frac{p}{d}\right)$$

nur durch einen gemeinschaftlichen Factor d des Moduls und der Glieder der Congruenz unterscheidet.

Somit sind alle Zahlen, welche unsere gegebene Congruenz

$$ax - b \equiv 0 \pmod{p}$$

befriedigen, durch die Werthe

$$x \equiv \alpha \left(\text{mod.}\ \frac{p}{d}\right)$$

vollkommen bestimmt.

Darauf gestützt, können wir nunmehr leicht zeigen wie viele Zahlen aus der Reihe

$$0,\ 1,\ 2,\ \ldots,\ p-1$$

die Congruenz

$$ax - b \equiv 0 \pmod{p}$$

befriedigen, wodurch sich nach der Definition die Anzahl der Lösungen dieser Congruenz bestimmen wird. Zu diesem Zwecke wollen wir eine allgemeine Formel für die Zahlen, welche die Congruenz

$$x \equiv \alpha \left(\text{mod.}\ \frac{p}{d}\right)$$

befriedigen, aufstellen.

Nach dem im § 11 Ausgesagten, finden wir die Formel für diese Zahlen in der Gestalt

$$x = \alpha - N\frac{p}{d}.$$

Da aber in dieser Formel, wie wir gesehen haben, $\alpha < \frac{p}{d}$ und nicht < 0 ist, so erhält man aus derselben Werthe von x, welche zwischen den Grenzen 0 und $p-1$ sich befinden, lediglich für folgende Werthe von N:

$$N = 0,\ -1,\ -2,\ \ldots,\ -(d-2),\ -(d-1).$$



Folglich sind unter den Zahlen der Reihe

$$0,\ 1,\ 2,\ \ldots,\ p-1,$$

folgende d Zahlen:

$$\alpha,\ \alpha+\frac{p}{d},\ \alpha+\frac{2p}{d},\ \ldots,\ \alpha+\frac{(d-1)p}{d}$$

und nur diese enthalten, welche die Congruenz

$$x \equiv \alpha \left(\text{mod.}\ \frac{p}{d}\right)$$

und somit auch die gegebene Congruenz

$$ax-b \equiv 0 \ (\text{mod.}\ p)$$

befriedigen.

Da nun die genannten d Zahlen aus der Reihe

$$0,\ 1,\ 2,\ \ldots,\ p-1$$

die Congruenz

$$ax-b \equiv 0 \ (\text{mod.}\ p),$$

befriedigen, so besitzt diese Congruenz nach Lehrsatz 14, wirklich die d Lösungen:

$$\left.\begin{array}{l} x \equiv \alpha \\ x \equiv \alpha+\frac{p}{d} \\ x \equiv \alpha+\frac{2p}{d} \\ \vdots \\ x \equiv \alpha+\frac{(d-1)p}{d} \end{array}\right\} (\text{mod.}\ p),$$

wie in dem Lehrsatze behauptet war.

So hat z. B. die Congruenz

$$15x-9 \equiv 0 \ (\text{mod.}\ 12),$$

in welcher der Coëfficient von x und der Modul den grössten gemeinschaftlichen Theiler 3 besitzen und zugleich das die Unbekannte x nicht enthaltende Glied durch 3 theilbar ist, wirklich drei Lösungen. Um dieselben zu finden, dividiren wir in der gegebenen Congruenz die Glieder und den Modul durch 3 und erhalten so die Congruenz

$$5x-3 \equiv 0 \ (\text{mod.}\ 4).$$

Auf Grund des im vorigen Paragraphen Auseinandergesetzten, finden wir die Lösung der letzteren in der Gestalt

$$x \equiv 3 \,.\, 5^{2^2 \frac{(2-1)}{2} - 1} \pmod{4},$$

oder

$$x \equiv 15 \pmod{4}.$$

Ersetzen wir die Zahl 15 durch ihren kleinsten positiven Rest in Bezug auf den Modul 4, so finden wir:

$$x \equiv 3 \pmod{4}.$$

Daraus entnehmen wir nun für die vorgelegte Congruenz

$$15x - 9 \equiv 0 \pmod{12}$$

die Lösungen:

$$\left.\begin{array}{l} x \equiv 3 \\ x \equiv 7 \\ x \equiv 11 \end{array}\right\} \pmod{12}.$$

Kapitel III.

Ueber allgemeine Congruenzen höheren Grades.

§ 17. Ueber die Befreiung von dem Coëfficienten der höchsten Potenz der Unbekannten.

In diesen Untersuchungen wollen wir uns auf die Betrachtung von Congruenzen beschränken, deren Modul eine Primzahl ist. Die allgemeine Gestalt der Congruenzen, mit welchen wir uns hier beschäftigen wollen, wird folgende sein:

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \ldots + Hx + S \equiv 0 \pmod{p},$$

wobei p eine Primzahl bedeutet und $A, B, C, \ldots, H, S$ irgend welche ganze Zahlen sind.

Bevor wir zur Untersuchung der Lösungen solcher Congruenzen schreiten, wollen wir die Bemerkung machen, dass man es immer bewirken kann, den Coëfficienten der höchsten Potenz von x auf Eins zu bringen. In der That kann man in einer Congruenz

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \ldots + Hx + S \equiv 0 \pmod{p}$$

solche Glieder immer weglassen, deren Coëfficienten durch p theilbar sind. Wenn z. B. C durch p theilbar ist, so werden wir, in unserer Bezeichnungsweise ausgedrückt, die Congruenz haben:

$$C \equiv 0 \pmod{p},$$

welche durch Multiplication mit x^{m-2} in

$$Cx^{m-2} \equiv 0 \pmod{p}$$

übergeht. Indem wir nun diese von der Congruenz

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \dots + Hx + S \equiv 0 \pmod{p}$$

subtrahiren, befreien wir die letztere von dem Gliede Cx^{m-2}.

Dasselbe kann offenbar mit jedem anderen Gliede geschehen, dessen Coëfficient durch p theilbar ist. Setzen wir nun voraus, die Congruenz

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \dots + Hx + S \equiv 0 \pmod{p}$$

sei bereits von allen solchen Gliedern, deren Coëfficienten Vielfache von p sind, befreit worden und Ax^m sei dabei das Glied mit der höchsten Potenz von x. In diesem Falle wird A, da es kein Vielfaches von der Primzahl p sein soll, relativ prim zum Modul p sein und es wird sich nach dem oben (§ 13, Lehrs. 15; vgl. auch § 15) Bewiesenen eine Zahl α finden lassen, für welche die Congruenz ersten Grades

$$A\alpha - 1 \equiv 0 \pmod{p}$$

befriedigt wird.

Multiplicirt man diese Congruenz nach und nach mit

$$Bx^{m-1},\ Cx^{m-2},\ \dots,\ Hx,\ S,$$

so erhält man die entsprechenden Congruenzen:

$$\left.\begin{array}{lll} AB\alpha x^{m-1} & - Bx^{m-1} & \equiv 0 \\ AC\alpha x^{m-2} & - Cx^{m-2} & \equiv 0 \\ & \vdots & \\ AH\alpha x & - Hx & \equiv 0 \\ AS\alpha & - S & \equiv 0 \end{array}\right\} \pmod{p} \quad . \quad . \quad (8a)$$

Addirt man alle diese Congruenzen zu der von uns betrachteten

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \dots + Hx + S \equiv 0 \pmod{p},$$

so erhält man:

$$Ax^m + AB\alpha x^{m-1} + AC\alpha x^{m-2} + \dots + AH\alpha x + AS\alpha \equiv 0 \pmod{p}.$$

Da aber A relativ prim zu p ist, so können wir die Glieder der Congruenz durch A dividiren, wodurch wir endlich die Congruenz

$$x^m + B\alpha x^{m-1} + C\alpha x^{m-2} + \dots + H\alpha x + S\alpha \equiv 0 \pmod{p}$$

erhalten, in welcher der Coëfficient der höchsten Potenz von x wirklich Eins ist, was zu bewirken war.

[Man kann aber leicht beweisen, dass unsere ursprüngliche Congruenz dieselben Lösungen hat, wie die, auf welche wir sie zurückgeführt haben. Denkt man sich nämlich in der Letzteren für x einen Werth $x = \beta$ gesetzt, welcher sie befriedigt, so wird sie offenbar auch durch $x = \beta$ befriedigt sein, wenn man dieselbe mit A multiplicirt haben wird. Unsere Congruenz wird aber auch durch $x = \beta$ noch befriedigt bleiben, nachdem man von derselben die Congruenzen (8a) subtrahirt haben wird; *weil die letzteren, sobald* α *so gewählt ist, dass* $A\alpha - 1 \equiv 0 \pmod{p}$ *befriedigt wird, alle für jeden Werth von* x *überhaupt, also auch für* $x = \beta$ *befriedigt werden.* Ebenso kann man umgekehrt schliessen, dass wenn die ursprüngliche Congruenz durch einen gewissen Werth $x = \gamma$ befriedigt wird, dieselbe es auch noch bleibt, nachdem man die Congruenzen (8a), welche für jeden Werth von x befriedigt werden, hinzu addirt, und auch nachdem man das Resultat durch die zum Modul p relative Primzahl A dividirt hat und es wird somit $x = \gamma$ auch die letzterhaltene Congruenz befriedigen. Die ursprüngliche Congruenz und diejenige, auf welche dieselbe immer zurückgeführt werden kann, haben somit genau dieselben Lösungen und unterscheiden sich bloss in der Form; und wir wählen daher die Form, wo der Coëfficient der höchsten Potenz von x Eins ist, welche durch unsere ferneren Betrachtungen die Eigenschaften der Congruenz besser beleuchten lassen wird].

So haben wir z. B., um die Congruenz

$$2x^3 + 3x + 7 \equiv 0 \pmod{11}$$

in eine andere umzuformen, in welcher der Coëfficient von x^3 gleich Eins werde, nur eine Zahl α zu finden, für welche die Congruenz ersten Grades

$$2\alpha - 1 \equiv 0 \pmod{11}$$

besteht. Eine solche Zahl α ist 6. Daranf bilden wir die Congruenzen:

$$\left.\begin{array}{l} 2.3.6x - 3x \equiv 0 \\ 2.7.6 \quad - 7 \quad \equiv 0 \end{array}\right\} \text{(mod. 11)}.$$

Haben wir diese zu unserer gegebenen Congruenz

$$2x^3 + 3x + 7 \equiv 0 \text{ (mod. 11)}$$

addirt und geordnet, so finden wir:

$$2x^3 + 2.3.6x + 2.6.7 \equiv 0 \text{ (mod. 11)};$$

woraus, nach Division durch 2, endlich die Congruenz

$$x^3 + 18x + 42 \equiv 0 \text{ (mod. 11)}$$

folgt, in welcher der Coëfficient der höchsten Potenz von x Eins ist.

---

§ 18. **Obere Grenze für die Anzahl der Lösungen.**

Wir beweisen in Bezug auf die Lösungen einer Congruenz höheren Grades folgenden

20. *Lehrsatz. Ist p eine Primzahl, so kann die Congruenz m^{ten} Grades*

$$x^m + Bx^{m-1} + Cx^{m-2} + \ldots + Hx + S \equiv 0 \text{ (mod. } p)$$

nicht mehr als m Lösungen haben.

Beweis. Um diesen Satz zu beweisen, bemerken wir, dass derselbe nach § 13 richtig ist für $m = 1$, d. h. für Congruenzen ersten Grades. Um die Richtigkeit des Satzes für einen beliebigen Grad zu beweisen, wollen wir zeigen, dass derselbe für Congruenzen vom Grade m richtig sein muss, wenn seine Richtigkeit für Congruenzen vom Grade $m-1$ erwiesen sein sollte.

Um uns davon zu überzeugen, wollen wir versuchen das Gegentheil zuzulassen, dass nämlich die Congruenz m^{ten} Grades

$$x^m + Bx^{m-1} + Cx^{m-2} + \ldots + Hx + S \equiv 0 \text{ (mod. } p)$$

mehr als m Lösungen habe, während jede Congruenz der-

selben Art vom Grade $m-1$ mehr als $m-1$ Lösungen nicht haben könne, und wir wollen die Unzulässigkeit einer solchen Annahme nachweisen.

Wir haben bereits gesehen, dass die Anzahl der Lösungen irgend einer Congruenz mit dem Modul p überhaupt durch die Anzahl der in der Reihe

$$0,\ 1,\ 2,\ \ldots.,\ p-1$$

enthaltenen Zahlen bestimmt wird, welche die Congruenz befriedigen. Daher kann die Congruenz

$$x^m + Bx^{m-1} + Cx^{m-2} + \ldots. + Hx + S \equiv 0 \pmod{p}$$

nur dann mehr als m Lösungen besitzen, wenn derselben mehr als m Zahlen aus der Reihe

$$0,\ 1,\ 2,\ \ldots.,\ p-1$$

genügen. Es mögen nun wirklich $m+1$ solcher Zahlen existiren und wir bezeichnen dieselben mit

$$a,\ a_1,\ a_2,\ \ldots.,\ a_m.$$

Wir greifen eine derselben, z. B. a heraus und durch die Differenz $x-a$ dividiren wir den Ausdruck linker Hand in unserer Congruenz

$$x^m + Bx^{m-1} + Cx^{m-2} + \ldots. + Hx + S$$

und erhalten den Quotienten, offenbar, in der Gestalt:

$$x^{m-1} + B_1x^{m-2} + C_1x^{m-3} + \ldots. + H_1x + S_1$$

und dazu noch als Rest eine gewisse Zahl R. Indem wir nun den Dividendus gleich setzen der Summe des Productes von Divisor und Quotienten plus dem Reste, erhalten wir:

$$x^m + Bx^{m-1} + Cx^{m-2} + \ldots. + Hx + S$$
$$= (x-a)(x^{m-1} + B_1x^{m-2} + C_1x^{m-3} + \ldots. + H_1x + S_1) + R.$$

Somit kann unsere Congruenz

$$x^m + Bx^{m-1} + Cx^{m-2} + \ldots. + Hx + S \equiv 0 \pmod{p}$$

in der Form

$$(x-a)(x^{m-1} + B_1x^{m-2} + C_1x^{m-3} + \ldots. + H_1x + S_1) + R \equiv 0 \pmod{p}$$

dargestellt werden. Setzen wir hierin $x = a$, wobei a der Voraussetzung gemäss eine der die Congruenz befriedigenden Zahlen sein soll, so finden wir für R die Congruenz

$$R \equiv 0 \pmod{p}$$

und indem wir diese letztere, von x vollkommen unabhängige, Congruenz von der vorhergehenden subtrahiren, erhalten wir unsere gegebene Congruenz, welche nach der Voraussetzung $(m+1)$ Lösungen haben soll, in der Gestalt:

$$(x-a)(x^{m-1}+B_1x^{m-2}+C_1x^{m-3}+\ldots+H_1x+S_1)\equiv 0 \pmod{p} \ldots (9)$$

Wir wollen nun zusehen, ob in der That dieser Congruenz $m+1$ Zahlen

$$a,\ a_1,\ a_2,\ \ldots,\ a_m,$$

welche in der Reihe

$$0,\ 1,\ 2,\ \ldots,\ p-1$$

enthalten sind, genügen können, wenn angenommen wird, dass eine Congruenz $m-1^{\text{ten}}$ Grades, wie

$$x^{m-1}+B_1x^{m-2}+C_1x^{m-3}+\ldots+H_1x+S_1\equiv 0 \pmod{p}$$

mehr als $m-1$ Lösungen nicht haben kann.

Hat letztere Congruenz nicht mehr als $m-1$ Lösungen, so können nicht alle aus der Reihe

$$0,\ 1,\ 2,\ \ldots,\ p-1$$

entnommenen m Zahlen

$$a_1,\ a_2,\ \ldots,\ a_m$$

der Congruenz Genüge leisten. Mag nun a_1 diejenige Zahl sein, welche der Congruenz *nicht* genügt; es wird dann der Ausdruck

$$a_1^{m-1}+B_1a_1^{m-2}+C_1a_1^{m-3}+\ldots+H_1a_1+S_1,$$

indem derselbe *nicht* congruent ist Null nach dem Modul p, eine Zahl repräsentiren, welche durch p nicht theilbar ist und welche folglich, da p eine Primzahl sein soll, relativ prim zu p ist. Dasselbe findet dann aber auch in Bezug auf die Differenz a_1-a statt, weil die Zahlen a_1

und a, indem jede von Ihnen nicht grösser als $p-1$ und nicht kleiner als Null vorausgesetzt war, in ihrer Differenz nicht eine Zahl liefern können, die durch p theilbar wäre. Folglich sind die Zahlen

$$a_1 - a,$$
$$a_1^{m-1} + B_1 a_1^{m-2} + C_1 a_1^{m-3} + \ldots + H_1 a_1 + S_1$$

relativ prim zu p; und mithin muss auch das Product derselben

$$(a_1 - a)(a_1^{m-1} + B_1 a_1^{m-2} + C_1 a_1^{m-3} + \ldots + H_1 a_1 + S_1)$$

relativ prim zu p sein, woraus, im Gegensatz zu der gemachten Voraussetzung, folgt, dass $x = a_1$ die Congruenz (9) nicht befriedigt; somit ist unsere versuchte Annahme: eine Congruenz m^{ten} Grades könne mehr als m Lösungen haben nicht möglich, was zu beweisen war.

Auf Grund dieses Satzes können wir folgenden allgemeineren Lehrsatz beweisen.

21. *Lehrsatz.* *Sind nicht alle Coëfficienten der allgemeinen Congruenz m^{ten} Grades*

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \ldots + Hx + S \equiv 0 \pmod{p}$$

durch p theilbar, so kann die Congruenz nicht mehr als m Lösungen haben.

Beweis. Wir haben in § 17 gesehen, dass in einer Congruenz

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \ldots + Hx + S \equiv 0 \pmod{p}$$

alle solche Glieder weggelassen werden können, deren Coëfficienten durch p theilbar sind. Durch eine solche Weglassung von Gliedern wird die Congruenz

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \ldots + Hx + S \equiv 0 \pmod{p},$$

wenn in derselben alle Coëfficienten $A, B, C, \ldots, H, S$, Vielfache von p sind auf die Identität

$$0 \equiv 0 \pmod{p}$$

zurückgeführt werden. Im anderen Falle wird die Congruenz

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \ldots + Hx + S \equiv 0 \pmod{p}$$

auf eine andere zurückgeführt werden, deren Coëfficienten durch p nicht theilbar sind. Verwandeln wir diese (nach § 17) in eine Form, in welcher der Coëfficient der höchsten Potenz Eins ist, so schliessen wir nach dem vorhergehenden Lehrsatze, dass die Congruenz nicht mehr Lösungen haben kann als Einheiten in dem höchsten Exponenten derselben enthalten sind; da aber die Congruenz, welche aus

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \ldots + Hx + S \equiv 0 \pmod{p}$$

durch weglassung irgend welcher Glieder erhalten wird, offenbar nicht von höherem als $m$ten Grade sein kann, so kann dieselbe nicht mehr als m Lösungen haben, was wir beweisen wollten.

---

§ 19. **Anwendung obigen Satzes auf den Beweis des Wilson'schen Theorems und anderer Eigenschaften der Zahlen.**

Auf Grund obigen Lehrsatzes können viele merkwürdige Eigenschaften der Zahlen bewiesen werden. Unter Anderem wollen wir z. B. folgenden Lehrsatz beweisen.

22. *Lehrsatz. Die Coëfficienten aller Potenzen von x in dem ausgerechneten und nach Potenzen von x geordneten Ausdruck*

$$(x-1)(x-2)(x-3)\ldots(x-(p-1)) - x^{p-1} + 1$$

sind alle durch p theilbar, wenn p eine Primzahl ist.

Beweis. Der Ausdruck

$$(x-1)(x-2)(x-3)\ldots(x-(p-1))$$

wird Null für die Werthe $x = 1, 2, 3, \ldots, p-1$; folglich befriedigen alle diese Werthe von x die Congruenz

$$(x-1)(x-2)(x-3)\ldots(x-(p-1)) \equiv 0 \pmod{p}.$$

Dieselben Werthe von x befriedigen aber, nach dem Fermat'schen Satze, die Congruenz

$$x^{p-1} - 1 \equiv 0 \pmod{p}.$$



Subtrahirt man diese letztere Congruenz von der vorhergehenden, so erhält man die neue Congruenz

$$(x-1)(x-2)(x-3)\dots(x-(p-1))-x^{p-1}+1\equiv 0 \pmod{p},$$

welche ebenfalls durch die Zahlen 1, 2, 3, ..., $p-1$ befriedigt wird, weil sie aus Congruenzen erhalten worden ist, welche einzeln durch dieselben Zahlen 1, 2, 3, ..., $p-1$ befriedigt werden.

Genügen aber der Congruenz

$$(x-1)(x-2)(x-3)\dots(x-(p-1))-x^{p-1}+1\equiv 0 \pmod{p}$$

die Zahlen 1, 2, 3, ..., $p-1$, so hat dieselbe $(p-1)$ Lösungen

$$\left.\begin{array}{l} x\equiv 1 \\ x\equiv 2 \\ x\equiv 3 \\ \;\vdots \\ x\equiv p-1 \end{array}\right\} \pmod{p}.$$

Nach dem vorhergehenden Lehrsatze ist aber dieses nur dann möglich, wenn sämmtliche Coëfficienten des ausgerechneten und nach Potenzen von x geordneten Ausdruckes

$$(x-1)(x-2)(x-3)\dots(x-(p-1))-x^{p-1}+1$$

einzeln durch p theilbar sind, weil sonst die Congruenz, welche offenbar $(p-2)^{\text{ten}}$ Grades ist, keine $p-1$ Lösungen besitzen könnte. Hiermit ist also unser Lehrsatz bewiesen.

Wir wollen nun zusehen, auf welche Congruenzen wir durch diesen Lehrsatz geführt werden.

Zu diesem Ende bemerken wir, dass der Ausdruck

$$(x-1)(x-2)(x-3)\dots(x-(p-1))-x^{p-1}+1$$

nach Ausführung der Multiplication und Anordnung der Glieder in

$$-(1+2+3+\dots+p-1)x^{p-2}+(1.2+1.3+\dots+2.3+\dots)x^{p-3}$$
$$-(1.2.3+1.2.4+\dots+2.3.4+\dots)x^{p-4}+\dots+(-1)^{p-1}(1.2.3\dots(p-1))+1$$

verwandelt wird; folglich werden nach dem bewiesenen Lehrsatze die Zahlen

$$1+2+3+\dots+(p-1),$$
$$1.2+1.3+\dots+2.3+\dots+(p-2)(p-1),$$
$$1.2.3+1.2.4+\dots+(p-3)(p-2)(p-1)$$
$$\dots\dots\dots\dots\dots\dots$$
$$(-1)^{p-1}1.2.3\dots(p-1)+1$$

Vielfache von p sein. In unserer Bezeichnungsweise heisst das: *es bestehen die Congruenzen:*

$$\left.\begin{array}{r} 1+2+3+\dots+(p-1)\equiv 0 \\ 1.2+1.3+\dots+(p-2)(p-1)\equiv 0 \\ 1.2.3+1.2.4+\dots+(p-3)(p-2)(p-1)\equiv 0 \\ \vdots \\ (-1)^{p-1}1.2.3\dots(p-1)+1\equiv 0 \end{array}\right\} \pmod{p}.$$

Alle diese Congruenzen finden somit statt für jede Primzahl p.

So hat man z. B. für $p=5$ wirklich:

$$\left.\begin{array}{r} 1+2+3+4\equiv 0 \\ 1.2+1.3+1.4+2.3+2.4+3.4\equiv 0 \\ 1.2.3+1.2.4+1.3.4+2.3.4\equiv 0 \\ 1.2.3.4+1\equiv 0 \end{array}\right\} \pmod{5}.$$

Besonders bemerkenswerth ist hier die letzte dieser Congruenzen, nämlich:

$$(-1)^{p-1}1.2.3\dots(p-1)+1\equiv 0 \pmod{p},$$

welche uns auf folgenden Lehrsatz führt, der unter dem Namen des „*Wilson'schen Lehrsatzes*" bekannt ist.

23. *Lehrsatz. Ist p eine Primzahl, so ist*

$$1.2.3\dots(p-1)+1\equiv 0 \pmod{p}.$$

Beweis. Die Primzahl p kann entweder 2, oder grösser als 2 sein. Im letzteren Falle muss dieselbe, als Primzahl, immer ungerade sein. Die für alle Primzahlen p gültige Congruenz

$$(-1)^{p-1}1.2.3\ldots.(p-1)+1\equiv 0 \pmod{p}$$

wird aber bei ungeradem p in

$$1.2.3\ldots.(p-1)+1\equiv 0 \pmod{p}$$

verwandelt.

Dieselbe Congruenz ist aber auch für $p = 2$ richtig, weil sie in diesem Falle in

$$1+1\equiv 0 \pmod{2},$$

übergeht, was offenbar richtig ist. Somit ist die Richtigkeit des Wilson'schen Satzes für alle Fälle bewiesen.

Es ist übrigens nicht schwer allgemeiner zu beweisen, dass *wenn m Zahlen $a_1, a_2, a_3, \ldots., a_m$, welche kleiner als p und nicht kleiner als Null sind, die Congruenz*

$$Ax^m+Bx^{m-1}+Cx^{m-2}+\ldots.+Lx+M\equiv 0 \pmod{p}$$

befriedigen, dann die Congruenzen

$$\left.\begin{aligned} -A(a_1+a_2+a_3+\ldots.+a_m) &\equiv B\\ A(a_1a_2+a_1a_3+\ldots.+a_{m-1}a_m &\equiv C\\ &\vdots\\ (-1)^{m-1}A(a_1a_2\ldots.a_{m-1}+\ldots.+a_2a_3\ldots.a_m) &\equiv L\\ (-1)^m A\,a_1a_2a_3\ldots.a_m &\equiv M \end{aligned}\right\} \pmod{p}$$

bestehen.

Denn die Werthe

$$x = a_1,\ a_2,\ a_3,\ \ldots.,\ a_m$$

machen den Ausdruck

$$A(x-a_1)(x-a_2)(x-a_3)\ldots.(x-a_m)$$

zu Null; folglich befriedigen dieselben Zahlen die Congruenz

$$A(x-a_1)(x-a_2)(x-a_3)\ldots.(x-a_m)\equiv 0 \pmod{p}.$$

Der Voraussetzung nach befriedigen aber dieselben Zahlen auch die Congruenz

$$Ax^m+Bx^{m-1}+Cx^{m-2}+\ldots.+Lx+M\equiv 0 \pmod{p};$$

folglich müssen dieselben Zahlen auch die Congruenz, welche als Differenz der beiden letzteren erhalten wird, nämlich:

$$A(x-a_1)(x-a_2)(x-a_3)\ldots(x-a_m)$$
$$-Ax^m-Bx^{m-1}-Cx^{m-2}-\ldots-Lx-M\equiv 0 \pmod{p}$$

befriedigen. Genügen aber dieser Congruenz m Zahlen $a_1, a_2, a_3, \ldots a_m$, welche aus der Reihe

$$0,\ 1,\ 2,\ \ldots, p-1$$

entnommen sind, so besitzt dieselbe m Lösungen, während ihr Grad niedriger als der m^{te} ist, indem das Glied mit x^m in dem Ausdrucke

$$A(x-a_1)(x-a_2)(x-a_3)\ldots(x-a_m)$$
$$-Ax^m-Bx^{m-1}-Cx^{m-2}-\ldots-Lx-M$$

wegfällt. Folglich müssen, nach Lehrsatz 21, alle Coëfficienten von x in dem ausgerechneten und geordneten Ausdrucke der linken Seite der Congruenz

$$A(x-a_1)(x-a_2)(x-a_3)\ldots(x-a_m)$$
$$-Ax^m-Bx^{m-1}-Cx^{m-2}-\ldots-Lx-M\equiv 0 \pmod{p}$$

einzeln durch p theilbar sein.

Es sind aber in dieser Congruenz die Coëfficienten von

$$x^{m-1},\ x^{m-2},\ \ldots,\ x,\ x^0$$

folgende:

$$\begin{array}{lr}
-A(a_1+a_2+a_3\ldots+a_m) & -B, \\
A(a_1a_2+a_1a_3+\ldots+a_{m-1}a_m) & -C, \\
\vdots & \\
(-1)^{m-1}A(a_1a_2\ldots a_{m-1}+\ldots+a_2a_3\ldots a_m) & -L, \\
(-1)^m A\, a_1a_2a_3\ldots a_m & -M.
\end{array}$$

Die Theilbarkeit dieser Ausdrücke durch p heisst aber in der von uns angenommenen Bezeichnungsweise:

$$\left.\begin{array}{rr} -A(a_1+a_2+a_3+\ldots+a_m) & -B\equiv 0 \\ A(a_1a_2+a_1a_3+\ldots+a_{m-1}a_m) & -C\equiv 0 \\ \vdots & \\ (-1)^{m-1}A(a_1a_2\ldots a_{m-1}+\ldots+a_2a_3\ldots a_m) & -L\equiv 0 \\ (-1)^m A\,a_1a_2a_3\ldots a_m & -M\equiv 0 \end{array}\right\}(\text{mod.}\,p),$$

woraus unmittelbar die Congruenzen

$$\left.\begin{array}{rr} -A(a_1+a_2+a_3+\ldots+a_m) & \equiv B \\ A(a_1a_2+a_1a_3+\ldots+a_{m-1}a_m) & \equiv C \\ \vdots & \\ (-1)^{m-1}A(a_1a_2\ldots a_{m-1}+\ldots+a_2a_3\ldots a_m) & \equiv L \\ (-1)^m A\,a_1a_2a_3\ldots a_m & \equiv M \end{array}\right\}(\text{mod.}\,p)$$

folgen, welche wir beweisen wollten.

So ergeben sich z. B. aus der Congruenz

$$x^3+2x^2+x-4\equiv 0\ (\text{mod. } 11),$$

welcher die drei Zahlen 1, 3, 5 genügen, die identischen Congruenzen für die Coëfficienten:

$$\left.\begin{array}{r} -(1+3+5)\equiv 2 \\ 1.3+1.5+3.5\equiv 1 \\ -1.3.5\equiv -4 \end{array}\right\}(\text{mod. } 11).$$

---

§ 20. Zurückführung einer Congruenz auf eine Form, in welcher der Grad kleiner wird als der Modul.

Wir haben bewiesen, dass eine Congruenz m^{ten} Grades

$$x^m+Bx^{m-1}+Cx^{m-2}+\ldots+Lx+M\equiv 0\ (\text{mod.}\,p)$$

nicht mehr als m Lösungen haben kann. Nunmehr wollen wir nachsehen, unter welchen Umständen eine solche Congruenz *auch nicht weniger* als m Lösungen hat. Dabei werden wir immer voraussetzen, dass der Grad m nicht grösser als $p-1$ ist. Damit aber diese Voraussetzung

nicht etwa als eine Einschränkung der Allgemeinheit betrachtet werde, wollen wir zuerst zeigen, dass eine allgemeine Congruenz

$$x^m + Bx^{m-1} + Cx^{m-2} + \ldots. + Lx + M \equiv 0 \pmod{p}$$

immer auf jene Form zurückgeführt werden kann.

24. *Lehrsatz. Ist p eine Primzahl, so kann die Congruenz m^{ten} Grades*

$$x^m + Bx^{m-1} + Cx^{m-2} + \ldots. + Lx + M \equiv 0 \pmod{p}$$

immer durch eine Congruenz $(p-1)^{ten}$ Grades

$$A_1 x^{p-1} + B_1 x^{p-2} + C_1 x^{p-3} + \ldots. + L_1 x + M_1 \equiv 0 \pmod{p}$$

ersetzt werden, wobei das Polynom

$$A_1 x^{p-1} + B_1 x^{p-2} + C_1 x^{p-3} + \ldots. + L_1 x + M_1$$

der Rest ist, welcher bei der Division des gegebenen Polynoms

$$x^m + Bx^{m-1} + Cx^{m-2} + \ldots. + Lx + M$$

durch

$$x^p - x$$

erhalten wird.

Beweis. Dividirt man das Polynom

$$x^m + Bx^{m-1} + Cx^{m-2} + \ldots. + Lx + M$$

durch $x^p - x$, so werden Quotient und Rest ganze Functionen mit ganzen Coëfficienten sein; dabei wird der Grad des Restes kleiner sein als der des Divisors $x^p - x$, folglich nicht grösser als $p-1$. Mag nun der Quotient bei dieser Division mit $\Phi(x)$ und der Rest mit

$$A_1 x^{p-1} + B_1 x^{p-2} + C_1 x^{p-3} + \ldots. + L_1 x + M_1$$

bezeichnet werden. Indem wir nun den Dividendus der Summe des Productes von Divisor und Quotienten plus dem Reste gleich setzen, erhalten wir:

$$x^m + Bx^{m-1} + Cx^{m-2} + \ldots. + Lx + M$$
$$= \Phi(x)(x^p - x) + A_1 x^{p-1} + B_1 x^{p-2} + C_1 x^{p-3} + \ldots + L_1 x + M_1 \quad (10)$$

Durch die Betrachtung dieser Gleichung kann man sich leicht überzeugen, dass die Congruenz

$$x^m + Bx^{m-1} + Cx^{m-2} + \ldots + Lx + M \equiv 0 \pmod{p}$$

der Congruenz

$$A_1 x^{p-1} + B_1 x^{p-2} + C_1 x^{p-3} + \ldots + L_1 x + M_1 \equiv 0 \pmod{p}$$

vollkommen identisch ist. Denn der Ausdruck $x^p - x$ ist für beliebige Werthe von x congruent Null nach dem Modul p; schreibt man nämlich

$$x^p - x = x\,(x^{p-1} - 1),$$

so sieht man sofort, dass wenn x ein Vielfaches von p ist, der erste Factor des Ausdruckes durch p theilbar wird und wenn x durch p nicht theilbar ist, so genügt der zweite Factor (nach dem Fermat'schen Satze) der Congruenz

$$x^{p-1} - 1 \equiv 0 \pmod{p}.$$

Daraus folgt, dass das Product

$$\Phi(x)\,(x^p - x)$$

für beliebige Werthe von x congruent ist Null nach dem Modul p.

Somit können wir von der linken Seite der Congruenz

$$x^m + Bx^{m-1} + Cx^{m-2} + \ldots + Lx + M \equiv 0 \pmod{p},$$

ohne ihre Gültigkeit zu beeinträchtigen, das Product

$$\Phi(x)\,(x^p - x)$$

subtrahiren, wodurch dieselbe die Gestalt

$$x^m + Bx^{m-1} + Cx^{m-2} + \ldots + Lx + M - \Phi(x)(x^p - x) \equiv 0 \pmod{p}$$

annimmt, und nach (10) kann dieselbe auf

$$A_1 x^{p-1} + B_1 x^{p-2} + C_1 x^{p-3} + \ldots + L_1 x + M_1 = 0 \pmod{p}$$

zurückgeführt werden, was zu beweisen war.

Dadurch ist der Schluss begründet, dass der Grad einer Congruenz mit dem Modul 2 immer bis auf 1 herabgesetzt, der Grad einer mit dem Modul 3 bis auf 2, einer mit dem Modul 5 bis auf 4 u. s. w. herabgesetzt werden kann.

So können wir z. B., wenn die Congruenz

$$x^5 + x^2 - 1 \equiv 0 \pmod{3}$$

gegeben ist, den Grad derselben bis auf 2 herabdrücken. Zu diesem Ende suchen wir den Rest der Division von $x^5 + x^2 - 1$ durch $x^3 - x$ auf. Da dieser Rest $x^2 + x - 1$ ist, so können wir die betrachtete Congruenz durch

$$x^2 + x - 1 \equiv 0 \pmod{3}$$

ersetzen.

---

§ 21. **Kriterium, zur Entscheidung ob eine Congruenz so viele Lösungen besitzt, als deren Grad Einheiten hat.**

Nachdem wir gezeigt haben, wie man den Grad einer Congruenz mit dem Modul p bis auf $p-1$ herabdrücken kann, wollen wir nunmehr zeigen, unter welchen Bedingungen eine Congruenz $m$ten Grades

$$x^m + Bx^{m-1} + Cx^{m-2} + \ldots + Lx + M \equiv 0 \pmod{p}$$

m Lösungen hat, wenn m nicht grösser als $p-1$ ist. Wir setzen hierbei den Coëfficienten der höchsten Potenz von x gleich Eins voraus, weil wir gesehen haben, dass man es bei jeder Congruenz so einrichten kann.

Nach folgenden Lehrsätzen wird man immer beurtheilen können, ob eine solche Congruenz so viele Lösungen als Einheiten in dem Exponenten ihres Grades vorhanden sind, hat, oder nicht.

25. *Lehrsatz. Hat die Congruenz*

$$x^m + Bx^{m-1} + Cx^{m-2} + \ldots + Lx + M \equiv 0 \pmod{p}$$

m Lösungen, so sind die Coëfficienten in dem Reste der Division von $x^p - x$ durch

$$x^m + Bx^{m-1} + Cx^{m-2} + \ldots + Lx + M$$

alle durch p theilbar.



Beweis. Wir bezeichnen mit $F(x)$ den Quotienten der Division von $x^p - x$ durch

$$x^m + Bx^{m-1} + Cx^{m-2} + \ldots\ldots + Lx + M$$

und mit $\varphi(x)$ den Rest dieser Division und erhalten, indem wir den Dividendus der Summe des Productes von Divisor und Quotienten plus dem Reste gleich setzen:

$$x^p - x = F(x)(x^m + Bx^{m-1} + Cx^{m-2} + \ldots. + Lx + M) + \varphi(x),$$

woraus

$$(11) \quad x^p - x - F(x)(x^m + Bx^{m-1} + Cx^{m-2} + \ldots. + Lx + M) = \varphi(x)$$

sich ergiebt.

Wir bilden nun die Congruenz

$$x^p - x - F(x)(x^m + Bx^{m-1} + Cx^{m-2} + \ldots. + Lx + M) \equiv 0 \pmod{p}$$

und beweisen, dass dieselbe, unter den gemachten Voraussetzungen, nicht weniger als m Lösungen hat. Dieses folgt daraus, dass der Ausdruck $x^p - x$, wie wir in § 20 gesehen haben, für beliebige Werthe von x congruent ist Null nach dem Modul p und was das Product

$$F(x)(x^m + Bx^{m-1} + Cx^{m-2} + \ldots. + Lx + M)$$

betrifft, so wird dasselbe für alle solche Werthe von x congruent Null nach dem Modul p, welche die Congruenz

$$x^m + Bx^{m-1} + Cx^{m-2} + \ldots. + Lx + M \equiv 0 \pmod{p}$$

befriedigen. Letztere Congruenz hat aber nach der Voraussetzung m Lösungen.

Somit hat die Congruenz

$$x^p - x - F(x)(x^m + Bx^{m-1} + Cx^{m-2} + \ldots. + Lx + M) \equiv 0 \pmod{p}$$

mindestens m Lösungen. Diese Congruenz ist aber nach (11) auf

$$\varphi(x) \equiv 0 \pmod{p}$$

zurückführbar, deren Grad kleiner als m ist; weil $\varphi(x)$ für uns den Rest der Division von $x^p - x$ durch

$$x^m + Bx^{m-1} + Cx^{m-2} + \ldots. + Lx + M$$

bedeutet.

Haben wir uns auf diese Weise von der Congruenz

$$\varphi(x) \equiv 0 \pmod{p}$$

einerseits überzeugt, dass dieselbe mindestens m Lösungen hat und andererseits, dass ihr Grad niedriger, als der $m$te ist, so schliessen wir nach Lehrsatz 21, dass die Coëfficienten in $\varphi(x)$ alle durch p theilbar sein müssen, worin der zu beweisende Satz bestand.

Wir wollen nunmehr den umgekehrten Lehrsatz beweisen.

26. *Lehrsatz.* *Sind in dem Reste der Division von $x^p - x$ durch*

$$x^m + Bx^{m-1} + Cx^{m-2} + \ldots + Lx + M$$

alle Coëfficienten Vielfache von p, so hat die Congruenz

$$x^m + Bx^{m-1} + Cx^{m-2} + \ldots + Lx + M \equiv 0 \pmod{p}$$

m Lösungen.

Beweis. Es mögen wieder $F(x)$ und $\varphi(x)$ den Quotienten, respective Rest bei der Division von $x^p - x$ durch

$$x^m + Bx^{m-1} + Cx^{m-2} + \ldots + Lx + M$$

bedeuten und in dem Reste $\varphi(x)$ sollen alle Coëfficienten, nach Voraussetzung, Vielfache von p sein. Dann wird für jeden Werth von x die Congruenz

$$\varphi(x) \equiv 0 \pmod{p} \quad \ldots\ldots \quad (12)$$

bestehen, während der Quotient $F(x)$ eine ganze Function $(p\text{-}m)$ten Grades von der Gestalt

$$F(x) = x^{p-m} + B_1 x^{p-m-1} + \ldots$$

sein wird.

Setzt man den Dividendus gleich der Summe des Productes von Divisor und Quotienten plus dem Reste, so findet man

$$x^p - x = F(x)(x^m + Bx^{m-1} + Cx^{m-2} + \ldots + Lx + M) + \varphi(x),$$

woraus

$$x^p - x - \varphi(x) = F(x)(x^m + Bx^{m-1} + Cx^{m-2} + \ldots + Lx + M)$$



folgt. Da aber nach (12) und nach dem oben über $x^p - x$ Auseinandergesetzten die linke Seite der letzten Gleichung, $x^p - x - \varphi(x)$ für alle Zahlen $0, 1, 2, \ldots, p-1$ congruent ist Null nach dem Modul p, so werden auch alle diese Zahlen die Congruenz

$$F(x)\,(x^m + Bx^{m-1} + Cx^{m-2} + \ldots + Lx + M) \equiv 0 \pmod{p}$$

befriedigen, weil die linke Seite derselben, nach dem eben Ausgeführten, mit der Differenz $x^p - x - \varphi(x)$ identisch ist.

Es genügen also alle p Zahlen $0, 1, 2, \ldots, p-1$ der Congruenz p^{ten} Grades

$$F(x)\,(x^m + Bx^{m-1} + Cx^{m-2} + \ldots + Lx + M) \equiv 0 \pmod{p},$$

welcher offenbar keine solche Zahl genügen kann, die nicht einer der beiden Congruenzen

$$F(x) \equiv 0 \pmod{p},$$
$$x^m + Bx^{m-1} + Cx^{m-2} + \ldots + Lx + M \equiv 0 \pmod{p}$$

genügen würde. Denn wenn z. B. der Werth $x = \alpha$ keine dieser letzten Congruenzen befriedigt, so werden sowohl $F(\alpha)$ als auch $\alpha^m + B\alpha^{m-1} + C\alpha^{m-2} + \ldots + L\alpha + M$ Zahlen sein, welche durch p nicht theilbar sind, d. h. (weil p selbst eine Primzahl ist) Zahlen, welche relativ prim sind zu p. Sind aber die Zahlen $F(\alpha)$ und

$$\alpha^m + B\alpha^{m-1} + C\alpha^{m-2} + \ldots + L\alpha + M$$

relativ prim zu p, so muss auch ihr Product

$$F(\alpha)\,(\alpha^m + B\alpha^{m-1} + C\alpha^{m-2} + \ldots + L\alpha + M)$$

eine Zahl repräsentiren, welche relativ prim zu p ist; und folglich kann die Congruenz

$$F(x)\,(x^m + Bx^{m-1} + Cx^{m-2} + \ldots + Lx + M) \equiv 0 \pmod{p}$$

durch $x = \alpha$ nicht befriedigt werden.

Es muss also jede der Zahlen $0, 1, 2, \ldots, p-1$ mindestens eine der beiden Congruenzen

$$F(x) \equiv 0\,; \quad x^m + Bx^{m-1} + Cx^{m-2} + \ldots + Lx + M \equiv 0 \pmod{p}$$

befriedigen.

Bezeichnen wir daher mit n die Anzahl derjenigen Zahlen der Reihe

$$0, 1, 2, \ldots, p-1,$$

welche die eine Congruenz

$$F(x) \equiv 0 \pmod{p}$$

und mit n' die Anzahl derjenigen Zahlen aus derselben Reihe, welche die andere Congruenz

$$x^m + Bx^{m-1} + Cx^{m-2} + \ldots + Lx + M \equiv 0 \pmod{p}$$

befriedigen, so ist jedenfalls die Summe

$$n + n' \text{ nicht kleiner als } p.$$

Dabei geben n und n' beziehungsweise die Anzahl der Lösungen der Congruenz

$$F(x) \equiv 0, \text{ resp. } x^m + Bx^{m-1} + Cx^{m-2} + \ldots + Lx + M \equiv 0 \pmod{p}$$

an, welche ja, wie wir öfter wiederholt haben, durch die Anzahl der Zahlen aus der Reihe 0, 1, 2, ..., $p-1$, die die betreffende Congruenz befriedigen, bestimmt wird. Folglich ist nach Lehrsatz 20

$$n' \text{ nicht grösser als } m, \text{ und } n \text{ nicht grösser als } p-m;$$

weil $F(x)$, wie wir gesehen haben eine Function $(p-m)^{\text{ten}}$ Grades in der Gestalt

$$x^{p-m} + B_1 x^{p-m-1} + \ldots$$

ist.

Es werden also die Zahlen n und n', welche resp. die Anzahl der Lösungen der Congruenzen

$$F(x) \equiv 0 \text{ und } x^m + Bx^{m-1} + Cx^{m-2} + \ldots + Lx + M \equiv 0 \pmod{p}$$

angeben, den Bedingungen

$$n + n' \geqq p; \quad n \leqq p - m; \quad n' \leqq m$$

zu genügen haben.

Eliminirt man n aus den ersten zwei dieser drei Bedingungen, so erhält man für n' die Bedingung

$$n' \geqq m,$$

welche in Verbindung mit der dritten der obigen Bedingungen

$$n' \leqq m$$

die Gleichung

$$n' = m$$

liefert, was bewiesen werden sollte.

Auf Grund der letzten zwei Lehrsätze sind wir nun immer im Stande zu entscheiden, ob eine gegebene Congruenz wirklich so viele Lösungen hat, als Einheiten in dem Exponenten ihres Grades vorhanden sind. Zu diesem Ende machen wir zuerst, nach der im § 17 gezeigten Methode, den Coëfficienten der höchsten Potenz in der gegebenen Congruenz gleich Eins und dividiren dann, indem wir mit p den Modul der Congruenz bezeichnen,

$$x^p - x$$

durch die linke Seite der gegebenen Congruenz. Sind dann in dem bei dieser Division sich ergebenden Reste sämmtliche Coëfficienten Vielfache von p, so schliessen wir nach dem letzten Lehrsatze, dass die gegebene Congruenz wirklich so viele Lösungen besitzt, als Einheiten in ihrem höchsten Exponenten vorhanden sind. Im entgegengesetzten Falle schliessen wir nach dem vorletzten Lehrsatze, dass die gegebene Congruenz so viele Lösungen nicht besitzt.

Um z. B. zu erfahren, ob die Congruenz

$$x^3 - x^2 - 2x \equiv 0 \pmod{5}$$

drei Lösungen hat, oder nicht, dividiren wir

$$x^5 - x$$

durch

$$x^3 - x^2 - 2x.$$

Da diese Division den Rest

$$5x^2 + 5x$$

ergiebt, in welchem beide Coëfficienten durch 5 theilbar sind, so schliessen wir, dass die gegebene Congruenz drei Lösungen hat. [In der That überzeugt man sich in diesem Falle, wo der Modul eine kleine Zahl 5 ist, durch einfaches Einsetzen für x die Werthe $x = 0, 1, 2. 3, 4,$

dass $x = 1$ und $x = 3$ die Congruenz nicht befriedigen; dagegen

$$x \equiv 0;\quad x \equiv 2;\quad x \equiv 4 \pmod{5}$$

die Lösungen wirklich sind.]

Dagegen liefert die Division von

$$x^5 - x$$

durch

$$x^3 + x^2 - 2$$

den Rest

$$x^2 - 3x + 2,$$

in welchem die Coëfficienten nicht theilbar sind durch 5, und wir schliessen daher, dass die Congruenz

$$x^3 + x^2 - 2 \equiv 0 \pmod{5}$$

weniger als drei Lösungen hat.

[In der That überzeugt man sich leicht, dass die Werthe

$$x = 0;\ x = 3;\ x = 4$$

die Congruenz nicht befriedigen, dagegen

$$x \equiv 1;\ x \equiv 2 \pmod{5}$$

Lösungen sind.]

Kapitel IV.

Ueber Congruenzen zweiten Grades.

§ 22. Zurückführung der vollständigen Congruenzen zweiten Grades auf die Congruenz von der Form
$$z^2 \equiv q \pmod{p}.$$

Die allgemeine Form einer Congruenz zweiten Grades ist

$$ax^2 + bx + c \equiv 0 \pmod{p}.$$

In zwei Fällen kann diese Congruenz auf Congruenzen ersten Grades zurückgeführt werden. *Erstens*, wenn $p = 2$ ist. In diesem Falle kann man nach Lehrsatz 24 den Grad einer Congruenz m^{ten} Grades überhaupt, also auch den Grad von

$$ax^2 + bx + c \equiv 0 \pmod{2}$$

bis auf 1 herabdrücken. Man dividirt hier die linke Seite durch $x^2 - x$ und ersetzt die gegebene Congruenz durch die ihr identische Congruenz ersten Grades

$$(a + b)\, x + c \equiv 0 \pmod{2}.$$

Zweitens kann man die gegebene Congruenz zweiten Grades

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

auf eine solche ersten Grades zurückführen, wenn a durch p theilbar ist; weil wir in diesem Falle die Congruenz

$$a \equiv 0 \pmod{p}$$

mit x^2 multipliciren und die dadurch erhaltene:

$$ax^2 \equiv 0 \pmod{p}$$

von der gegebenen

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

subtrahiren können, wodurch wir eine Congruenz ersten Grades

$$bx + c \equiv 0 \pmod{p}$$

erhalten, welche mit der ursprünglichen identisch ist.

Also, wenn entweder $p = 2$ ist, oder a ein Multiplum von p, kann die Congruenz zweiten Grades

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

auf eine ersten Grades zurückgeführt werden, welche wir lösen können. Wir wenden uns nun zu dem Falle, dass p nicht gleich 2 und a kein Vielfaches von p ist und wollen uns vorerst, zur Vereinfachung der Untersuchung, auf die Annahme beschränken, dass p eine Primzahl ist.

Wir werden nun zeigen worauf die Lösung der Congruenz

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

in diesem Falle zurückzuführen ist.

Da p, nach der Voraussetzung, eine Primzahl und von 2 verschieden und a kein Multiplum von p ist, so wird $4a$ relativ prim zu p sein; folglich wird, wie man sich leicht überzeugen kann, die Congruenz

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

mit

$$4a(ax^2 + bx + c) \equiv 0 \pmod{p}$$

identisch sein.

In der That ist die zweite der beiden Congruenzen in der ersten enthalten; weil wir immer, ohne eine Congruenz zu beeinträchtigen, die Glieder derselben mit einer beliebigen Zahl multipliciren dürfen. Umgekehrt ist aber die erste Congruenz in der zweiten enthalten, indem sie aus derselben durch eine erlaubte Weglassung des Factors $4a$ hervorgeht, — eine erlaubte Weglassung, weil $4a$ relativ prim zu p vorausgesetzt worden ist.

Die Congruenz

$$4a\,(ax^2 + bx + c) \equiv \text{(mod. } p)$$

kann man aber so schreiben:

$$(2ax + b)^2 - b^2 + 4ac \equiv 0 \text{ (mod. } p).$$

Hieraus leiten wir die Congruenz

$$z^2 \equiv b^2 - 4ac \text{ (mod. } p)$$

ab, indem wir

$$z = 2ax + b$$

setzen.

Daraus ersehen wir, dass die Lösung der Congruenz

$$ax^2 + bx + c \equiv 0 \text{ (mod. } p)$$

auf die Lösung von

$$z^2 \equiv b^2 - 4ac \text{ (mod. } p)$$

und auf die Bestimmung von x durch die Gleichung

$$2ax + b = z$$

zurückgeführt wird.

Was nun die Bestimmung von x aus der Gleichung

$$2ax + b = z$$

betrifft, nachdem z bereits durch die Lösung der Congruenz

$$z^2 \equiv b^2 - 4ac \text{ (mod. } p)$$

gefunden ist, so ist diese Bestimmung auf die Lösung einer Congruenz ersten Grades zurückzuführen.

Nach dem, was wir über die Lösungen von Congruenzen in der Form $f(x) \equiv 0$ (mod. p), in welchen $f(x)$ eine ganze Function von x mit ganzen Coëfficienten bedeutet, bemerkt haben, wird nämlich die Lösung der Congruenz

$$z^2 \equiv b^2 - 4ac \text{ (mod. } p)$$

jedenfalls durch eine oder mehrere Congruenzen in der Gestalt

$$z \equiv \alpha \text{ (mod. } p)$$

dargestellt werden. Folglich werden wir, um x zu bestimmen, welches mit z durch die Gleichung

$$2ax + b = z$$

verbunden ist, die Congruenz

$$2ax + b \equiv \alpha \pmod{p}$$

erhalten.

Diese Congruenz *ersten Grades* zu lösen, haben wir bereits gelernt. Wir bemerken zugleich, dass dieselbe, unter den gemachten Voraussetzungen *immer* eine Lösung besitzen wird; weil nämlich hier die beiden Zahlen $2a$ und p relativ prim zu einander sind.

Somit besteht die Schwierigkeit der Lösung der allgemeinen Congruenz zweiten Grades

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

lediglich in der Auffindung der Lösung der specielleren Congruenz

$$z^2 \equiv b^2 - 4ac \pmod{p};$$

mit dieser letzteren wollen wir uns nunmehr eingehender beschäftigen. Wir werden dieselbe in der Form

$$z^2 \equiv q \pmod{p}$$

schreiben, indem wir, Kürze halber,

$$b^2 - 4ac = q$$

setzen werden.

Indem wir nun die Congruenz

$$z^2 \equiv q \pmod{p}$$

näher betrachten, bemerken wir sofort, dass dieselbe, falls

$$q \equiv 0 \pmod{p}$$

ist, durch

$$z \equiv 0 \pmod{p}$$

befriedigt wird. Man kann sich auch leicht überzeugen, dass in diesem Falle $z \equiv 0 \pmod{p}$ die einzig mögliche Lösung der Congruenz $z^2 \equiv q \pmod{p}$ sein wird. Denn, sobald q congruent Null nach dem Modul p ist, drückt ja die Congruenz $z^2 \equiv q \pmod{p}$ nichts Anderes aus, als dass z^2 durch p theilbar ist. Da aber p, als Primzahl, nicht durch das Quadrat irgend einer Zahl theilbar sein kann, so muss die Theilbarkeit von z^2 durch p, nach Lehrsatz 6, die Theilbarkeit von z selbst durch p zur Voraussetzung haben, was wir aber durch

$$z \equiv 0 \pmod{p}$$

ausdrücken.



Somit besitzt die Congruenz

$$z^2 \equiv q \pmod{p},$$

wenn q congruent Null nach dem Modul p ist, die *einzige* Lösung

$$z \equiv 0 \pmod{p}.$$

Gehen wir nun zu dem Falle über, dass q in Bezug auf den Mod. p nicht congruent Null ist. In diesem Falle findet in Betreff der Lösungen der Congruenz $z^2 \equiv q \pmod{p}$ folgender Lehrsatz statt.

27. *Lehrsatz. Ist q nach dem Modul p nicht congruent Null, so hat die Congruenz*

$$z^2 \equiv q \pmod{p}$$

entweder gar keine Lösung, oder sie besitzt deren zwei.

Beweis. Wir haben gesehen, dass eine Congruenz $f(x) \equiv 0 \pmod{p}$ überhaupt genau so viele Lösungen besitzt, als es Zahlen unter denjenigen der Reihe $0, 1, 2, \ldots, p-1$ giebt, welche die Congruenz befriedigen. Darnach ist es aber leicht zu beweisen, dass die Annahme, die Congruenz

$$z^2 \equiv q \pmod{p}$$

habe *nur eine Lösung*, unmöglich ist, wenn nicht

$$q \equiv 0 \pmod{p}$$

ist.

Es mag, in der That, a diejenige Zahl aus der Reihe $0, 1, 2, \ldots, p-1$ sein, welche die Congruenz $z^2 \equiv q \pmod{p}$ befriedigt. Die Zahl a kann nicht Null sein: da die Substitution von $z = 0$ in $z^2 \equiv q \pmod{p}$ die Congruenz $0 \equiv q \pmod{p}$ abgeben würde, was gegen die Annahme wäre. Es kann somit a nur eine der Zahlen $1, 2, \ldots, p-1$ sein.

Es ist aber leicht einzusehen, dass wenn die Congruenz $z^2 \equiv q \pmod{p}$ durch die Zahl a befriedigt wird, dieselbe auch durch $p-a$ befriedigt werden muss; weil $(p-a)^2$, als eine mit $p^2 - 2ap + a^2$ identische Zahl, offenbar congruent ist a^2 nach mod. p. Es wird also $p-a$ immer dann eine zweite Lösung der Congruenz $z^2 \equiv q \pmod{p}$

liefern, wenn die Zahl $p - a$ *erstens* unter den Zahlen $0, 1, 2, \ldots, p-1$ enthalten und *zweitens* von a verschieden sein wird. *Ersteres* folgt aber aus dem Umstande, dass a nicht grösser als p und nicht kleiner als 1 ist; während die zweite Bedingung deshalb hier erfüllt sein muss, weil sonst

$$p - a = a, \text{ also } p = 2a$$

sich ergeben würde, was unmöglich ist, da die von 2 verschiedene Primzahl p keine gerade Zahl sein kann.

Befindet sich also unter den Zahlen der genannten Reihe *eine* Zahl, welche die Congruenz $z^2 \equiv q \pmod{p}$ befriedigt, so wird sich darunter zugleich auch noch eine *zweite* Zahl befinden, welche ebenfalls die genannte Congruenz befriedigt. Folglich ist es nicht möglich, dass diese Congruenz *nur eine* Lösung haben sollte. Da sie aber, als eine Congruenz zweiten Grades, auch nicht *mehr* als *zwei* Lösungen haben kann, so kann dieselbe nur *entweder zwei Lösungen*, *oder gar keine* besitzen, was wir beweisen wollten.

---

§ 23. **Ueber die Existenz der Lösungen der Congruenz** $z^2 \equiv q \pmod{p}$.

Wir wollen uns jetzt mit der Untersuchung derjenigen Kriterien beschäftigen, nach denen man entscheiden kann, ob die Congruenz $z^2 \equiv q \pmod{p}$, wenn nicht $q \equiv 0 \pmod{p}$ ist, zwei Lösungen besitzt, oder gar keine.

Auf Grund der in § 21 bewiesenen Lehrsätze ist es nun leicht zu erkennen, ob die Congruenz

$$z^2 - q \equiv 0 \pmod{p}$$

zwei Lösungen besitzt, oder nicht. Wir haben zu diesem Zwecke den Rest zu finden, welcher bei der Division von $z^p - z$ durch $z^2 - q$ erhalten wird. Um diesen Rest leichter finden zu können, schreiben wir den Dividendus $z^p - z$ in der Form

$$z\left[(z^2)^{\frac{p-1}{2}}-q^{\frac{p-1}{2}}\right]+z\left[q^{\frac{p-1}{2}}-1\right]$$

und bemerken, dass der Ausdruck

$$(z^2)^{\frac{p-1}{2}}-q^{\frac{p-1}{2}}$$

durch z^2-q theilbar ist. Folglich wird der Ausdruck

$$z\left[q^{\frac{p-1}{2}}-1\right]$$

der gesuchte Rest der Division von z^p-z durch z^2-q sein.

Daraus schliessen wir nach Lehrsatz 26, dass die Congruenz

$$z^2 \equiv q \pmod{p}$$

zwei Lösungen besitzt, wenn

$$q^{\frac{p-1}{2}}-1$$

durch p theilbar ist, oder in unserer angenommenen Ausdrucksweise, wenn die Congruenz

$$q^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

stattfindet.

Wird diese Congruenz nicht erfüllt, ist also $q^{\frac{p-1}{2}}-1$ kein Vielfaches von p, so schliessen wir nach Lehrsatz 25, dass die Congruenz $z^2 \equiv q \pmod{p}$ keine zwei Lösungen und somit auch gar keine Lösung besitzt; weil diese Congruenz nach Lehrsatz 27 entweder zwei Lösungen, oder gar keine zulassen kann.

Wir haben somit das Kriterium gewonnen:

Die Congruenz

$$z^2 \equiv q \pmod{p}$$

besitzt zwei Lösungen, oder gar keine, je nachdem die Congruenz

$$q^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

stattfindet, oder nicht.

Im ersteren Falle werden wir sagen: die Congruenz

$$z^2 \equiv q \pmod{p}$$

ist möglich; im entgegengesetzten Falle — sie sei unmöglich.

Wir erinnern hier noch daran, dass das eben erhaltene Kriterium unter der gemachten Voraussetzung gewonnen wurde, dass p eine von 2 verschiedene Primzahl und q eine beliebige, positive, oder negative, durch p nicht theilbare Zahl sei.

Beispiel. Um zu erkennen, ob die Congruenz

$$z^2 \equiv 3 \pmod{5}$$

Lösungen hat, oder nicht, erheben wir 3 zur $\frac{5-1}{2}$ten oder 2ten Potenz. Indem wir nun finden, dass 3^2 nach dem Modul 5 nicht congruent ist 1, schliessen wir, dass die Congruenz $z^2 \equiv 3 \pmod{5}$ keine Lösungen hat; mit andern Worten, dass diese Congruenz unmöglich ist; [durch Einsetzung der Werthe 0, 1, 2, 3, 4*) kann man sich von der Unmöglichkeit leicht überzeugen].

Dagegen überzeugen wir uns, dass die Congruenz

$$z^2 \equiv 2 \pmod{7}$$

zwei Lösungen besitzt, indem wir finden, dass

$$2^{\frac{7-1}{2}} = 8$$

nach dem Modul 7 congruent 1 ist; [in der That wird unsere Congruenz durch $z = 3$ und $z = 4 = 7 - 3$ befriedigt und $z \equiv 3$; $z \equiv 4 \pmod{7}$ sind also die zwei Lösungen derselben.]

---

§ 24. Ueber das Symbol $\left(\frac{q}{p}\right)$.

Sind p und q keine sehr grossen Zahlen, so ist es nicht schwer zu erkennen, ob die Congruenz

[* Es ist nur nöthig für $z = 1$ und $z = 2$ zu prüfen, weil 0 ausgeschlossen ist und 3; 4 die Zahlen 2, resp. 1 zu 5 ergänzen.]

$$q^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

stattfindet, oder nicht. Diese Erkenntniss wird dagegen sehr schwer, wenn p und q grosse Zahlen sind. Wir wollen nun zeigen, wie man sich, ohne den Werth von $q^{\frac{p-1}{2}}$ zu berechnen, überzeugen kann, ob die Congruenz $q^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ erfüllbar ist, oder nicht, um dadurch zu entscheiden, ob die Congruenz $z^2 \equiv q \pmod{p}$ Lösungen besitzt, oder nicht. Zu diesem Zwecke wollen wir zeigen, dass wenn q durch p nicht theilbar und p eine von 2 verschiedene Primzahl ist — und das waren ja unsere gemachten Voraussetzungen —, die Zahl $q^{\frac{p-1}{2}}$ jedenfalls eine der beiden Congruenzen

$$\left.\begin{aligned} q^{\frac{p-1}{2}} &\equiv 1 \\ q^{\frac{p-1}{2}} &\equiv -1 \end{aligned}\right\} \pmod{p}$$

befriedigen muss.

Denn, wenn keine von diesen beiden Congruenzen befriedigt sein sollte, so würde weder die Zahl $q^{\frac{p-1}{2}} - 1$, noch die Zahl $q^{\frac{p-1}{2}} + 1$ durch p theilbar sein und folglich müsste jede dieser Zahlen, da p selbst Primzahl ist, relativ prim zu p sein. Wären aber beide Zahlen

$$q^{\frac{p-1}{2}} - 1 \text{ und } q^{\frac{p-1}{2}} + 1$$

relativ prim zu p, so müsste auch ihr Product

$$\left(q^{\frac{p-1}{2}} - 1\right)\left(q^{\frac{p-1}{2}} + 1\right) = q^{p-1} - 1$$

relativ prim zu p sein, was nicht wahr sein kann, weil nach dem *Fermat*'schen Satze die Differenz $q^{p-1} - 1$ durch

p theilbar sein muss. Folglich wird eine der beiden Congruenzen

$$q^{\frac{p-1}{2}} \equiv 1; \quad q^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

jedenfalls erfüllt sein.

Man kann sich aber andererseits leicht überzeugen, dass diese Congruenzen nicht beide gleichzeitig bestehen können. Denn die Zulassung beider würde

$$1 \equiv -1 \pmod{p} \text{ und somit } 2 \equiv 0 \pmod{p}$$

ergeben, was unmöglich ist; weil p, als eine nach Voraussetzung von 2 verschiedene Primzahl, kein Theiler von 2 sein kann.

Aus unserer Auseinandersetzung folgt, dass die Möglichkeit der Congruenz $z^2 \equiv q \pmod{p}$ durch dasjenige Vorzeichen bestimmt wird, welches man in der rechten Seite der Congruenz

$$q^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$$

zu nehmen hat, damit dieselbe befriedigt werde. Wird dieselbe mit dem Vorzeichen $+$ befriedigt, so lässt die Congruenz $z^2 \equiv q \pmod{p}$ Lösungen zu und man nennt in diesem Falle die Zahl q einen *quadratischen Rest* der Zahl p. Im entgegengesetzten Falle, wenn nämlich die Congruenz

$$q^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$$

mit dem Vorzeichen $-$ befriedigt wird, lässt die Congruenz $z^2 \equiv q \pmod{p}$ keine Lösung zu und man nennt dann die Zahl q *quadratischen Nichtrest* von p.

Man ist ferner, um die Schreibweise abzukürzen, übereingekommen, anstatt zu schreiben: p und q befriedigen die Congruenz

$$q^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

was, wie wir gesehen haben, ein Kriterium ist für die Möglichkeit der Congruenz

$$z^2 \equiv q \pmod{p},$$

kürzer zu schreiben:

$$\left(\frac{q}{p}\right) = 1;$$

im entgegengesetzten Falle, wenn $q^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, schreibt man

$$\left(\frac{q}{p}\right) = -1.$$

Nach dieser Bezeichnungsweise bedeutet das Symbol $\left(\frac{q}{p}\right)$ die Zahl 1, mit demjenigen der beiden Vorzeichen $\pm$ genommen, mit welchem dieselbe der Congruenz

$$q^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$$

genügt. Folglich wird die Bedeutung des genannten Symbols durch die Congruenz

$$q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod{p}$$

und die gleichzeitige Bedingung, dass der Zahlwerth von

$$\left(\frac{q}{p}\right)$$

immer 1 ist, vollkommen bestimmt sein.

Beispiel. Wir haben oben gesehen, dass die Congruenz

$$q^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

für $q = 2$ und $p = 7$ befriedigt ist; folglich wird nach unserer Bezeichnungsweise

$$\left(\frac{2}{7}\right) = 1$$

sein. Dagegen fanden wir oben, dass $3^{\frac{5-1}{2}}$, bezüglich den Modul 5 congruent ist -1; folglich ist

$$\left(\frac{3}{5}\right) = -1.$$

Auf diese Weise schliessen wir aus

$$\left(\frac{2}{7}\right) = 1,$$

dass die Lösung der Congruenz $z^2 \equiv 2 \pmod{7}$ möglich ist und nennen die Zahl 2 quadratischen Rest von 7. Dagegen folgern wir aus der Gleichung

$$\left(\frac{3}{5}\right) = -1$$

die Unmöglichkeit der Congruenz $z^2 \equiv 3 \pmod{5}$ und die Zahl 3 wird daher quadratischer Nichtrest von 5 sein.

---

§ 25. Eigenschaften des Symbols $\left(\frac{q}{p}\right)$.

Nachdem wir die Bedeutung des Symbols $\left(\frac{q}{p}\right)$ bestimmt haben, wollen wir zur Entwickelung seiner Eigenschaften schreiten und zunächst folgenden Lehrsatz beweisen.

28. *Lehrsatz. Das Symbol* $\left(\frac{1}{p}\right)$ *hat den Werth* 1 *und das Symbol* $\left(\frac{-1}{p}\right)$ *den Werth* $(-1)^{\frac{p-1}{2}}$.

Beweis. Wir haben gesehen, dass das Symbol $\left(\frac{q}{p}\right)$ immer die Congruenz

$$q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod{p}$$

befriedigt. Setzen wir hierin hintereinander $q = 1$ und $q = -1$, so erhalten wir

$$1 \equiv \left(\frac{1}{p}\right); \quad (-1)^{\frac{p-1}{2}} \equiv \left(\frac{-1}{p}\right) \pmod{p},$$

oder, was dasselbe ist:

$$1-\left(\frac{1}{p}\right)\equiv 0;\quad (-1)^{\frac{p-1}{2}}-\left(\frac{-1}{p}\right)\equiv 0 \text{ (mod. } p).$$

Da aber der Zahlwert beider Symbole

$$\left(\frac{1}{p}\right) \text{ und } \left(\frac{-1}{p}\right)$$

jedenfalls 1 ist, so werden die Differenzen

$$1-\left(\frac{1}{p}\right) \text{ und } (-1)^{\frac{p-1}{2}}-\left(\frac{-1}{p}\right),$$

falls nicht $\left(\frac{1}{p}\right) = 1$ und $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ wäre, entweder auf 2, oder auf -2 führen. Nun kann aber weder 2, noch -2 bezüglich Modul p congruent Null sein, da p eine von 2 verschiedene Primzahl ist. Folglich ist die Annahme, es seien nicht

$$\left(\frac{1}{p}\right) = 1 \text{ und } \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}},$$

unzulässig, wodurch unser Lehrsatz bewiesen ist.

Beispiele. Aus unserem Lehrsatze erhalten wir, dass

$$\left(\frac{1}{5}\right) = 1;\ \left(\frac{-1}{5}\right) = 1;\ \left(\frac{-1}{11}\right) = -1,$$

wovon man sich auch leicht überzeugen kann.

29. *Lehrsatz. Bedeutet Q das Product der Zahlen*

$$q_1,\ q_2,\ \ldots,\ q_n,$$

so ist

$$\left(\frac{Q}{p}\right) = \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right)\ldots\left(\frac{q_n}{p}\right).$$

Beweis. Die Symbole $\left(\frac{Q}{p}\right);\ \left(\frac{q_1}{p}\right),\ \left(\frac{q_2}{p}\right),\ \ldots,\ \left(\frac{q_n}{p}\right)$ befriedigen, wie wir gesehen haben, die Congruenzen

$$\left.\begin{array}{l} Q^{\frac{p-1}{2}} \equiv \left(\frac{Q}{p}\right); \\ q_1^{\frac{p-1}{2}} \equiv \left(\frac{q_1}{p}\right), \quad q_2^{\frac{p-1}{2}} \equiv \left(\frac{q_2}{p}\right), \ldots, \; q_n^{\frac{p-1}{2}} \equiv \left(\frac{q_n}{p}\right) \end{array}\right\} \text{(mod. } p\text{).}$$

Multiplicirt man alle diese letzteren Congruenzen, mit Ausnahme der ersten, gliedweise mit einander, so erhält man:

$$q_1^{\frac{p-1}{2}} \, q_2^{\frac{p-1}{2}} \ldots . q_n^{\frac{p-1}{2}} \equiv \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right) \ldots . \left(\frac{q_n}{p}\right) \text{ (mod. } p\text{),}$$

oder, was dasselbe ist:

$$[q_1 . q_2 \ldots . q_n]^{\frac{p-1}{2}} \equiv \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right) \ldots \left(\frac{q_n}{p}\right) \text{ (mod. } p\text{).}$$

Nach der Voraussetzung ist aber $q_1 \, q_2 \ldots . q_n = Q$, folglich geht die vorhergehende Congruenz in

$$Q^{\frac{p-1}{2}} \equiv \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right) \ldots . \left(\frac{q_n}{p}\right) \text{ (mod. } p\text{)}$$

über. Aus dieser Congruenz, zusammen mit der allerersten der obigen Congruenzen, nämlich:

$$Q^{\frac{p-1}{2}} \equiv \left(\frac{Q}{p}\right) \text{ (mod. } p\text{),}$$

erhalten wir dann

$$\left(\frac{Q}{p}\right) \equiv \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right) \ldots . \left(\frac{q_n}{p}\right) \text{ (mod. } p\text{),}$$

oder, anders geschrieben:

$$\left(\frac{Q}{p}\right) - \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right) \ldots \left(\frac{q_n}{p}\right) \equiv 0 \text{ (mod. } p\text{).}$$

Da nun der Zahlwerth der Symbole

$$\left(\frac{Q}{p}\right); \; \left(\frac{q_1}{p}\right), \; \left(\frac{q_2}{p}\right), \ldots, \; \left(\frac{q_n}{p}\right)$$

jedenfalls 1 ist, so würde die Differenz der beiden Ausdrücke

$$\left(\frac{Q}{p}\right) \text{ und } \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right) \cdots \left(\frac{q_n}{p}\right),$$

falls dieselben nicht einander gleich wären, entweder 2, oder -2 werden. Weder in dem einen, noch in dem andern Falle, würde aber die vorhergehende Congruenz bestehen können; weil p von 2 verschieden ist. Es ist also die Annahme, es seien die beiden Ausdrücke

$$\left(\frac{Q}{p}\right) \text{ und } \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right) \cdots \left(\frac{q_n}{p}\right)$$

nicht einander gleich, unzulässig und somit ist unser Lehrsatz bewiesen.

Auf Grund dieses Lehrsatzes wird die Bestimmung des Symbols $\left(\frac{Q}{p}\right)$, wenn Q eine zusammengesetzte Zahl ist, auf die Bestimmnng der Symbole

$$\left(\frac{q_1}{p}\right), \left(\frac{q_2}{p}\right), \cdots \left(\frac{q_n}{p}\right)$$

zurückgeführt, wobei $q_1, q_2, \ldots, q_n$ die in Q enthaltenen Primzahlen bedeuten.

Beispiele. Um die Symbole $\left(\frac{15}{7}\right)$; $\left(\frac{30}{101}\right)$ zu bestimmen, findet man:

$$\left(\frac{15}{7}\right) = \left(\frac{3}{7}\right)\left(\frac{5}{7}\right); \quad \left(\frac{30}{101}\right) = \left(\frac{2}{101}\right)\left(\frac{3}{101}\right)\left(\frac{5}{101}\right).$$

Als speciellen Fall des letzten Lehrsatzes können wir auch die Richtigkeit der Gleichung

$$\left(\frac{q^n}{p}\right) = \left(\frac{q}{p}\right)^n$$

behaupten. Man braucht, um diese Gleichung zu beweisen, nur in dem oben bewiesenen Lehrsatze alle Grössen $q_1, q_2, \ldots, q_n$ gleich q zu setzen. Es geht in diesem Falle die Gleichung

$$\left(\frac{Q}{p}\right) = \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right) \cdots \left(\frac{q_n}{p}\right)$$

in

$$\left(\frac{Q}{p}\right) = \left(\frac{q}{p}\right)^n$$

und Q, welches dem Producte $q_1\, q_2 \ldots q_n$ gleich sein soll, in q^n über.

Beispiele. Wir finden auf diese Weise:

$$\left(\frac{27}{5}\right) = \left(\frac{3^3}{5}\right) = \left(\frac{3}{5}\right)^3; \quad \left(\frac{32}{7}\right) = \left(\frac{2^5}{7}\right) = \left(\frac{2}{7}\right)^5.$$

In dem noch specielleren Falle, wenn $n = 2$ ist, geht

$$\left(\frac{q^n}{p}\right) = \left(\frac{q}{p}\right)^n \text{ in } \left(\frac{q^2}{p}\right) = \left(\frac{q}{p}\right)^2$$

über. Da nun das Quadrat von $\left(\frac{q}{p}\right)$, gleichviel, ob $\left(\frac{q}{p}\right)$ gleich $+1$, oder -1 ist, immer 1 sein wird, so erhalten wir:

$$\left(\frac{q^2}{p}\right) = 1.$$

Diese Eigenschaft des Symbols $\left(\frac{Q}{p}\right)$ kann zu bedeutenden Vereinfachungen dienen, wenn es sich um die Bestimmung des Werthes desselben handelt. Nach dem oben bewiesenen Lehrsatze hat man

$$\left(\frac{Nq^2}{p}\right) = \left(\frac{N}{p}\right)\left(\frac{q^2}{p}\right);$$

setzt man darin für $\left(\frac{q^2}{p}\right)$ seinen Werth aus der vorhergehenden Gleichung, so findet man:

$$\left(\frac{Nq^2}{p}\right) = \left(\frac{N}{p}\right).$$

Auf Grund dieser Gleichung kann man bei der Bestimmung des Werthes von $\left(\frac{Q}{p}\right)$ immer in Q jeden Factor weglassen, welcher ein vollständiges Quadrat bildet.

Beispiele. 1. Der Werth von $\left(\frac{45}{7}\right)$ ist derselbe wie der von $\left(\frac{5}{7}\right)$.

2. Der Werth von $\left(\frac{8}{5}\right)$ ist dem von $\left(\frac{2}{5}\right)$ gleich.

Bevor wir weiter gehen, bemerken wir, dass auf Grund der über das Symbol $\left(\frac{q}{p}\right)$ bewiesenen Sätze, der Werth von $\left(\frac{-q}{p}\right)$ vermittelst $\left(\frac{q}{p}\right)$ durch die Gleichung

$$\left(\frac{-q}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{q}{p}\right)$$

bestimmt wird.

Betrachtet man, in der That, $(-q)$ als das Product von (-1) und q, so findet man, infolge des letzten Lehrsatzes,

$$\left(\frac{-q}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right).$$

Setzt man darin für den einen Factor $\left(\frac{-1}{p}\right)$ seinen im 28. Lehrsatze gewonnenen Werth, so erhält man

$$\left(\frac{-q}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{q}{p}\right),$$

was zu beweisen war.

Beispiele. Wir finden auf diese Weise:

$$\left(\frac{-3}{5}\right) = (-1)^{\frac{5-1}{2}} \left(\frac{3}{5}\right) = \left(\frac{3}{5}\right);$$

$$\left(\frac{-2}{7}\right) = (-1)^{\frac{7-1}{2}} \left(\frac{2}{7}\right) = -\left(\frac{2}{7}\right).$$

30. *Lehrsatz. Sind q und q_1 einander nach dem Modul p congruent, so ist*

$$\left(\frac{q}{p}\right) = \left(\frac{q_1}{p}\right).$$

Beweis. Nach der Voraussetzung sind die Zahlen

q und q_1 nach Modul p einander congruent. Erhebt man beide Seiten der Congruenz

$$q \equiv q_1 \pmod{p}$$

zur $\frac{p-1}{2}$ten Potenz, so erhält man:

$$q^{\frac{p-1}{2}} \equiv q_1^{\frac{p-1}{2}} \pmod{p}.$$

Die einzelnen Symbole $\left(\frac{q}{p}\right)$, $\left(\frac{q_1}{p}\right)$ befriedigen aber die Congruenzen

$$q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right); \quad q_1^{\frac{p-1}{2}} \equiv \left(\frac{q_1}{p}\right) \pmod{p}.$$

Folglich ergiebt sich aus der vorhergehenden Congruenz:

$$\left(\frac{q}{p}\right) \equiv \left(\frac{q_1}{p}\right) \pmod{p},$$

oder

$$\left(\frac{q}{p}\right) - \left(\frac{q_1}{p}\right) \equiv 0 \pmod{p}.$$

Da nun der Zahlwerth sowohl von $\left(\frac{q}{p}\right)$ als von $\left(\frac{q_1}{p}\right)$ immer 1 ist, so kann der Werth der linken Seite der letzten Congruenz, falls nicht die Werthe von $\left(\frac{q}{p}\right)$ und $\left(\frac{q_1}{p}\right)$ einander gleich wären, nur entweder $+2$, oder -2 sein, was unmöglich ist, da p von 2 verschieden ist. Folglich müssen die beiden genannten Symbole denselben Werth haben; was wir beweisen wollten.

Beispiel. Man findet demgemäss:

$$\left(\frac{23}{7}\right) = \left(\frac{23-7}{7}\right) = \left(\frac{23-2.7}{7}\right) = \left(\frac{23-3.7}{7}\right) = \left(\frac{2}{7}\right).$$

Wir schliessen aus dem obigen Lehrsatze, dass das Symbol $\left(\frac{q}{p}\right)$ dem Symbole $\left(\frac{r}{p}\right)$ gleich ist, wenn r den Rest bei der Division von q durch p bedeutet; weil der

Rest, wie wir in § 8 bemerkt haben, immer dem Dividendus congruent ist, wenn der Divisor als Modul genommen wird. Indem wir also in $\left(\frac{q}{p}\right)$ die Zahl q durch den Rest der Division von q durch p ersetzen, erhalten wir anstatt $\left(\frac{q}{p}\right)$, wenn $q > p$, das Symbol $\left(\frac{r}{p}\right)$, wobei $r < p$ ist.

---

§ 26. Ausdrücke, welche den Werth des Symbols $\left(\frac{q}{p}\right)$ bestimmen. Folgerungen aus denselben: 1. Die Bestimmung von $\left(\frac{2}{p}\right)$; 2. das Reciprocitätsgesetz zweier Primzahlen.

Die obigen Lehrsätze können uns, wie wir gesehen haben, dazu dienen, den Werth irgend eines Symbols $\left(\frac{Q}{p}\right)$ auf den Werth eines einfacheren Symbols $\left(\frac{q}{p}\right)$ zurückzuführen, wobei q eine positive Primzahl, welche kleiner als p ist, bedeutet. Was nun die Bestimmung des Werthes eines solchen Symbols $\left(\frac{q}{p}\right)$ betrifft, wenn q eine positive Primzahl und kleiner als p ist, so wird dieselbe sich durch folgende Lehrsätze begründen lassen.

[Wir wollen jetzt eine Bezeichnungsweise erklären, welche zur Enthüllung vieler merkwürdigen Eigenschaften der Zahlen Manches beigetragen hat und von welcher wir im Folgenden Gebrauch machen werden.

Man bezeichnet die in einer Grösse λ enthaltene grösste ganze Zahl dadurch, dass man vor diese Grösse λ den Buchstaben E (entier) setzt, also $E\lambda$. So bedeutet z. B. $E\frac{37}{5}$ die Zahl 7, weil die grösste in $\frac{37}{5}$ enthaltene ganze Zahl 7 ist.]

31. *Lehrsatz.* *Versteht man unter $E\lambda$ die Grösste in irgend einer gegebenen Grösse λ enthaltene ganze Zahl, so ist der Werth*

des Symbols $\left(\frac{q}{p}\right)$ [*wenn p eine ungerade Primzahl und q kein Vielfaches von p ist,*] *genau dargestellt durch die Gleichung*

$$\left(\frac{q}{p}\right) = (-1)^{E\frac{2q}{p} + E\frac{4q}{p} + \cdots + E\frac{(p-1)q}{p}}.$$

Beweis. Man kann sich zunächst leicht überzeugen, dass man immer, wenn p ungerade ist und a irgend eine positive Zahl, eine bestimmte positive Zahl z finden kann, welche kleiner als $\frac{p}{2}$ ist und die Congruenz

$$z \equiv (-1)^{E\frac{2a}{p}} a \pmod{p} \quad . \quad . \quad . \quad . \quad . \quad (13)$$

befriedigt.

Denn diese Congruenz geht, wenn $E\frac{2a}{p}$ eine gerade Zahl ist, einfach in

$$z \equiv a \pmod{p}$$

über. Da aber in diesem Falle $\frac{1}{2} E\frac{2a}{p}$ eine ganze Zahl ist, so wird $a - \frac{1}{2} p E\frac{2a}{p}$ eine ganze Zahl sein, welche, für z gesetzt, die Congruenz

$$z \equiv a \pmod{p}$$

offenbar befriedigt. Diese Zahl, welche auch in der Form

$$\frac{p}{2}\left(\frac{2a}{p} - E\frac{2a}{p}\right)$$

geschrieben werden kann, ist positiv und kleiner als $\frac{p}{2}$; weil nach der Bedeutung von $E\frac{2a}{p}$ die Differenz

$$\frac{2a}{p} - E\frac{2a}{p}$$

immer kleiner als 1 und nicht kleiner als 0 sein wird.

Es bleibt uns also nur noch der Fall übrig, wenn

$E\frac{2a}{p}$ eine ungerade Zahl ist. In diesem Falle geht die Congruenz (13) in

$$z \equiv -a \pmod{p}$$

über.

Ist aber $E\frac{2a}{p}$ ungerade, so wird

$$\frac{1 + E\frac{2a}{p}}{2}$$

eine ganze Zahl sein und wir werden die vorhergehende Congruenz befriedigen, wenn wir für z den Werth

$$z = \tfrac{1}{2} p \left(1 + E\frac{2a}{p}\right) - a$$

setzen. Diese Zahl, welche man auch so schreiben kann:

$$\frac{p}{2}\left[1 - \left(\frac{2a}{p} - E\frac{2a}{p}\right)\right],$$

ist offenbar positiv und nicht grösser als $\frac{p}{2}$; weil die Differenz

$$\frac{2a}{p} - E\frac{2a}{p},$$

wie schon bemerkt, immer kleiner als 1 und niemals kleiner als 0 ist.

Haben wir uns nun überzeugt, dass man immer den Bedingungen

$$z \equiv (-1)^{E\frac{2a}{p}} a \pmod{p}; \quad 0 \lesseqgtr z < \frac{p}{2}$$

Genüge leisten kann, so wollen wir beziehungsweise mit

$$z_1, \; z_2, \; \ldots, \; z_{\frac{p-1}{2}}$$

diejenigen Zahlen bezeichnen, welche den obigen Bedingungen genügen, wenn man für a die Werthe

$$a = q; \; a = 2q; \; \ldots.; \; a = \frac{p-1}{2} q$$

setzt. Dann werden die Congruenzen

$$\left.\begin{array}{ll} z_1 & \equiv (-1)^{E\frac{2q}{p}} q \\ z_2 & \equiv (-1)^{E\frac{4q}{p}} 2q \\ & \vdots \\ z_{\frac{p-1}{2}} & \equiv (-1)^{E\frac{(p-1)q}{p}} \frac{p-1}{2} q \end{array}\right\} (\text{mod.}\, p) \quad \ldots (14)$$

bestehen, welche, gliedweise miteinander multiplicirt, die Congruenz

$$z_1\, z_2 \ldots z_{\frac{p-1}{2}} \equiv (-1)^S\, 1 \,.\, 2 \ldots \frac{(p-1)}{2}\, q^{\frac{p-1}{2}} (\text{mod.}\, p) \,.\,. (15),$$

wobei

$$S = E\frac{2q}{p} + E\frac{4q}{p} + \ldots + E\frac{(p-1)q}{p},$$

ergeben. Man kann sich nun leicht überzeugen, dass das Product $z_1\, z_2 \ldots z_{\frac{p-1}{2}}$ dem Producte $1 \,.\, 2 \ldots \frac{p-1}{2}$ gleich ist. Zu diesem Zwecke bemerken wir, dass die Zahlen $z_1, z_2, \ldots, z_{\frac{p-1}{2}}$, indem sie alle kleiner als $\frac{p}{2}$ und nicht kleiner als 0 sind, keine anderen Werthe als die in

$$0,\ 1,\ 2,\ \ldots,\ \frac{p-1}{2}$$

enthaltenen annehmen können. Dann bemerken wir ferner, dass keine unter ihnen den Werth Null haben kann; weil sonst aus der obigen Congruenz folgen würde, dass das Product

$$1 \,.\, 2 \ldots . \frac{p-1}{2}$$

durch p theilbar wäre, während die Zahlen $1, 2, \ldots, \frac{p-1}{2}$

offenbar relativ prim zu p sind. Folglich können die Zahlen $z_1, z_2, \ldots, z_{\frac{p-1}{2}}$ keine anderen Werthe, als

$$1,\ 2,\ \ldots,\ \frac{p-1}{2}$$

haben. Es ist aber auch leicht einzusehen, dass keine zwei unter den Zahlen $z_1, z_2, \ldots, z_{\frac{p-1}{2}}$ einander gleich sein können. Denn würden etwa z_m und z_μ einander gleich sein, während m und μ irgend zwei in der Reihe $1, 2, \ldots, \frac{p-1}{2}$ enthaltene Zahlen bedeuten sollen, so würde sich aus den in (14) enthaltenen Congruenzen

$$\left.\begin{aligned} z_m &\equiv (-1)^{E\frac{2qm}{p}} mq \\ z_\mu &\equiv (-1)^{E\frac{2q\mu}{p}} \mu q \end{aligned}\right\} \pmod{p}$$

die Congruenz

$$(-1)^{E\frac{2qm}{p}} mq \equiv (-1)^{E\frac{2q\mu}{p}} \mu q \pmod{p}$$

ergeben.

Diese Congruenz, welche nach Division durch die zu p relative Primzahl q in

$$(-1)^{E\frac{2qm}{p}} m \equiv (-1)^{E\frac{2q\mu}{p}} \mu \pmod{p}$$

übergeht, ist aber offenbar unmöglich; weil aus derselben die Theilbarkeit der Differenz

$$(-1)^{E\frac{2qm}{p}} m - (-1)^{E\frac{2q\mu}{p}} \mu$$

durch p folgen würde. Diese Differenz hat aber einen der vier Werthe

$$m + \mu;\quad -(m + \mu);\quad m - \mu;\quad -(m - \mu)$$

und da m und μ zwei von einander verschiedene Zahlen aus der Reihe $1, 2, \ldots, \frac{p-1}{2}$ bedeuten, so ist ihre

Summe kleiner als p und ihre Differenz ist von Null verschieden, folglich kann weder die Summe, noch die Differenz von m und μ durch p theilbar sein.

Auf diese Weise haben wir uns überzeugt, dass unter den Zahlen

$$z_1,\ z_2,\ \ldots,\ z_{\frac{p-1}{2}}$$

keine anderen als die aus der Reihe

$$1,\ 2,\ \ldots,\ \frac{p-1}{2}$$

entnommenen enthalten sein können und zwar kann jede von ihnen sich nur einmal darunter vorfinden; da aber beide Reihen aus gleich viel Gliedern bestehen, so müssen auch *alle* Zahlen der zweiten Reihe in der ersten Reihe enthalten sein. Es bestehen somit die Reihen

$$z_1,\ z_2,\ \ldots,\ z_{\frac{p-1}{2}}$$

$$1,\ 2,\ \ldots,\ \frac{p-1}{2}$$

aus ein und denselben Zahlen und zwar so, dass jede Zahl in jeder Reihe einmal vorkommt und somit ist das Product aller Glieder der ersten Reihe dem Producte aller Glieder der zweiten Reihe gleich.

Haben wir uns nun davon überzeugt, so können wir in (15) das Product $z_1 z_2 \ldots z_{\frac{p-1}{2}}$ durch $1 \,.\, 2 \ldots . \frac{p-1}{2}$ ersetzen und dann beide Seiten der Congruenz (15) durch die Zahlen $1,\ 2,\ \ldots,\ \frac{p-1}{2}$, welche relativ prim zu p sind, dividiren und erhalten dann

$$1 \equiv q^{\frac{p-1}{2}} (-1)^{E\frac{2q}{p} + E\frac{4q}{p} + \ldots + E\frac{(p-1)q}{p}} \pmod{p}.$$

Multipliciren wir beide Seiten dieser Congruenz mit

$$(-1)^{E\frac{2q}{p} + E\frac{4q}{p} + \ldots + E\frac{(p-1)q}{p}}$$

und bemerken, dass (—1), erhoben zur Potenz

$$2\left[E\frac{2q}{p}+E\frac{4q}{p}+\ldots+E\frac{(p-1)q}{p}\right],$$

jedenfalls 1 wird, so finden wir:

$$(-1)^{E\frac{2q}{p}+E\frac{4q}{p}+\ldots+E\frac{(p-1)q}{p}} \equiv q^{\frac{p-1}{2}} \pmod{p}.$$

Nach der Bedeutung des Symbols $\left(\frac{q}{p}\right)$ hat man nun

$$q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) (\text{mod.}\, p),$$

welche Congruenz, zusammen mit der vorhergehenden, endlich die Congruenz

$$\left(\frac{q}{p}\right) - (-1)^{E\frac{2q}{p}+E\frac{4q}{p}+\ldots+E\frac{(p-1)q}{q}} \equiv 0 \pmod{p}$$

liefert. Aus dieser Congruenz folgt aber die Gleichung

$$\left(\frac{q}{p}\right) = (-1)^{E\frac{2q}{p}+E\frac{4q}{p}+\ldots+E\frac{(p-1)q}{p}},$$

weil sonst die linke Seite der Congruenz entweder 2, oder —2 bedeuten würde und in beiden Fällen könnte die Theilbarkeit durch die ungerade Primzahl p nicht statthaft sein. Dadurch ist der Lehrsatz bewiesen; und wir sind nunmehr im Stande den Werth von $\left(\frac{q}{p}\right)$ zu berechnen, ohne die Zahl q auf die Potenz $\frac{p-1}{2}$ zu erheben.

Beispiel. Um den Werth des Symbols $\left(\frac{5}{11}\right)$ zu berechnen, erhalten wir zunächst:

$$\left(\frac{5}{11}\right) = (-1)^{E\frac{2.5}{11}+E\frac{4.5}{11}+E\frac{6.5}{11}+E\frac{8.5}{11}+E\frac{10.5}{11}}.$$

Bemerkt man nun, dass

$$\left.\begin{aligned} E\frac{2.5}{11} &= E\frac{10}{11} = 0; \\ E\frac{4.5}{11} &= E\frac{20}{11} = 1; \\ E\frac{6.5}{11} &= E\frac{30}{11} = 2; \\ E\frac{8.5}{11} &= E\frac{40}{11} = 3; \\ E\frac{10.5}{11} &= E\frac{50}{11} = 4; \end{aligned}\right\} \begin{aligned} &\text{folglich:} \\ &E\frac{2.5}{11} + E\frac{4.5}{11} + \ldots + E\frac{10.5}{11} \\ &= 0 + 1 + 2 + 3 + 4 = 10, \end{aligned}$$

so erhalten wir aus der obigen Gleichung

$$\left(\frac{5}{11}\right) = (-1)^{10} = 1.$$

Aus der oben begründeten, für jede Zahl q, welche kein Vielfaches von p ist, gültigen Gleichung zur Bestimmung des Werthes eines jeden Symbols $\left(\frac{q}{p}\right)$ kann man noch eine einfachere Gleichung herleiten, welche zur Bestimmung des Werthes von $\left(\frac{a}{p}\right)$ dienen soll, wenn a ungerade ist.

Zu diesem Zwecke wollen wir in der Gleichung

$$\left(\frac{q}{p}\right) = (-1)^{E\frac{2q}{p} + E\frac{4q}{p} + \ldots + E\frac{(p-1)q}{p}}$$

für q den Werth $q = \frac{1}{2}(a + p)$ setzen, wobei a, ebenso wie p, ungerade sein soll, und erhalten:

$$\left(\frac{\frac{1}{2}(a+p)}{p}\right) = (-1)^{E\frac{a+p}{p} + E\frac{2a+2p}{p} + \ldots + E\frac{\frac{p-1}{2}a + \frac{p-1}{2}p}{p}}$$

Multipliciren wir beide Seiten dieser Gleichung mit $\left(\frac{2}{p}\right)$, so finden wir:

$$\left(\frac{2}{p}\right)\left(\frac{\frac{1}{2}(a+p)}{p}\right)=\left(\frac{2}{p}\right)(-1)^{E\frac{a+p}{p}+E\frac{2a+2p}{p}+\ldots+E\frac{\frac{p-1}{2}a+\frac{p-1}{2}p}{p}}$$

Nach Lehrsatz 29 ist aber das Product $\left(\frac{2}{p}\right)\left(\frac{\frac{1}{2}(a+p)}{p}\right)$ dem einfacheren Symbole

$$\left(\frac{2\cdot\frac{1}{2}(a+p)}{p}\right)=\left(\frac{a+p}{p}\right)$$

gleich, welches seinerseits nach Lehrsatz 30 dem Symbole $\left(\frac{a}{p}\right)$ gleich ist. Folglich erhalten wir aus der obigen Gleichung:

$$\left(\frac{a}{p}\right)=\left(\frac{2}{p}\right)(-1)^{E\frac{a+p}{p}+E\frac{2a+2p}{p}+\ldots+E\frac{\frac{p-1}{2}a+\frac{p-1}{2}p}{p}}.$$

Nun ist aber

$$E\frac{a+p}{p}=E\left(\frac{a}{p}+1\right)=1+E\frac{a}{p},$$

$$E\frac{2a+2p}{p}=E\left(\frac{2a}{p}+2\right)=2+E\frac{2a}{p},$$

$$\vdots$$

$$E\frac{\frac{p-1}{2}a+\frac{p-1}{2}p}{p}=E\left(\frac{\frac{p-1}{2}a}{p}+\frac{p-1}{2}\right)=\frac{p-1}{2}+E\frac{\frac{p-1}{2}a}{p};$$

folglich wird:

$$\left(\frac{a}{p}\right)=\left(\frac{2}{p}\right)(-1)^{1+2+\ldots+\frac{p-1}{2}+E\frac{a}{p}+E\frac{2a}{p}+\ldots+E\frac{\frac{p-1}{2}a}{p}}.$$

Setzt man hierin für die Summe der arithmetischen Progression

$$1+2+\ldots+\frac{p-1}{2}$$

ihren Werth

$$\frac{\frac{p-1}{2}\left(\frac{p-1}{2}+1\right)}{2} = \frac{p^2-1}{8},$$

so verwandelt sich die obige Gleichung in

$$\left(\frac{a}{p}\right) = \left(\frac{2}{p}\right)(-1)^{\frac{p^2-1}{8}+E\frac{a}{p}+E\frac{2a}{p}+\dots+E\frac{\frac{p-1}{2}a}{p}} \qquad (16)$$

Aus dieser, für jede ungerade Zahl a, welche kein Vielfaches von p ist, gültigen Gleichung können wir zunächst den Werth des Symbols $\left(\frac{2}{p}\right)$ leicht erhalten. Setzen wir nämlich $a = 1$ und berücksichtigen die Werthe

$$\left(\frac{1}{p}\right) = 1;\ E\frac{1}{p} = 0,\ E\frac{2}{p} = 0, \dots, E\frac{\frac{p-1}{2}}{p} = 0,$$

so finden wir:

$$1 = \left(\frac{2}{p}\right)(-1)^{\frac{p^2-1}{8}},$$

woraus wir für das Symbol $\left(\frac{2}{p}\right)$ den Werth

$$\left(\frac{2}{p}\right) = (-1)^{-\frac{p^2-1}{8}}$$

erhalten.

Tragen wir nun diesen Werth von $\left(\frac{2}{p}\right)$ in (16) ein, so erhalten wir zu Lehrsatz 31 den

Zusatz I. *Ist a ungerade und kein Vielfaches von p, so ist*

$$\left(\frac{a}{p}\right) = (-1)^{E\frac{a}{p}+E\frac{2a}{p}+\dots+E\frac{\frac{1}{2}(p-1)a}{p}} \quad \dots (17).$$

Diese Gleichung ist derjenigen ähnlich, welche wir für $\left(\frac{q}{p}\right)$ im obigen Lehrsatze (31) hergeleitet haben, mit dem einzigen Unterschiede, dass hier die hinter dem Zeichen

E stehenden Zahlen nur halb so gross sind als die entsprechenden dort.

Beiläufig haben wir auch die Gleichung, die wir als *Zusatz* II

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

hervorheben, gefunden, welche zur Bestimmung von $\left(\frac{q}{p}\right)$ nur dienen wird, wenn q gleich 2, oder ein Vielfaches von 2 ist.

Auf Grund dieser Gleichung kann man behaupten, dass $\left(\frac{2}{p}\right) = 1$ ist, wenn $p = 8n \pm 1$; dagegen $\left(\frac{2}{p}\right) = -1$, wenn $p = 8n \pm 3$.

Setzen wir in der That in der obigen Gleichung anstatt p hintereinander $8n \pm 1$ und $8n \pm 3$, so erhalten wir:

$$\left(\frac{2}{8n \pm 1}\right) = (-1)^{\frac{(8n\pm1)^2-1}{8}} = (-1)^{8n^2 \pm 2n} = 1,$$

$$\left(\frac{2}{8n \pm 3}\right) = (-1)^{\frac{(8n\pm3)^2-1}{8}} = (-1)^{8n^2 \pm 6n - 1} = -1,$$

welches Resultat wir in folgendem Lehrsatz zusammenfassen:

32. *Lehrsatz. Ist* $p = 8n \pm 1$, *so ist* $\left(\frac{2}{p}\right) = 1$; *ist aber*

$p = 8n \pm 3$, *so ist* $\left(\frac{2}{p}\right) = -1$.

Beispiel. Man findet leicht:

$$\left(\frac{2}{17}\right) = 1; \quad \left(\frac{2}{13}\right) = -1.$$

Auf Grund der Gleichung (17) können wir noch einen anderen Lehrsatz beweisen, welcher ebenfalls sich auf die Bestimmung des Werthes von $\left(\frac{q}{p}\right)$ bezieht; derselbe besteht in Folgendem.

33. *Lehrsatz.* *Ist a ungerade und kleiner als p, so ist:*

$$\left(\frac{a}{p}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{p-1}{2} - E\frac{p}{a} - E\frac{2p}{a} - \dots - E\frac{\frac{1}{2}(a-1)p}{a}}.$$

Beweis. Wir haben in (17) für die Bestimmung von $\left(\frac{a}{p}\right)$, wenn a ungerade ist, die Gleichung erhalten:

$$\left(\frac{a}{p}\right) = (-1)^{E\frac{a}{p} + E\frac{2a}{p} + \dots + E\frac{\frac{1}{2}(p-1)a}{p}}.$$

Wir wollen nun zusehen, welche Werthe die Ausdrücke

$$E\frac{a}{p},\ E\frac{2a}{p},\ \dots,\ E\frac{\frac{1}{2}(p-1)a}{p}$$

haben, wenn a kleiner als p vorausgesetzt wird.

Den kleinsten Werth hat offenbar das erste Glied dieser Reihe, $E\frac{a}{p}$, während das letzte Glied $E\frac{\frac{1}{2}(p-1)a}{p}$ den grössten Werth besitzt. Da nun der Bruch $\frac{a}{p}$ kleiner als 1 ist, so ist $E\frac{a}{p} = 0$. Was nun den Ausdruck $E\frac{\frac{1}{2}(p-1)a}{p}$ betrifft, so kann man denselben auch so schreiben:

$$E\left(\frac{a}{2} - \frac{a}{2p}\right),\ \text{oder auch}\ E\left(\frac{a-1}{2} + \frac{p-a}{2p}\right),$$

in welcher Form man sofort übersieht, dass derselbe den Werth

$$\frac{a-1}{2}$$

hat; weil $\frac{a-1}{2}$ eine ganze Zahl ist und $\frac{p-a}{2p}$ ein positiver, echter Bruch ist, indem $a < p$ vorausgesetzt war.

Somit haben die Glieder der Reihe

$$E\frac{a}{p},\ E\frac{2a}{p},\ \dots,\ E\frac{\frac{1}{2}(p-1)a}{p}$$

ihrer Anordnung nach steigende Werthe von 0, bis $\frac{a-1}{2}$. Um ihre Summe zu berechnen, müssen wir genau bestimmen, wie viele von den Gliedern die Werthe

$$0,\ 1,\ 2,\ \dots,\ \frac{a-1}{2}$$

haben.

Zu diesem Zwecke bestimmen wir zunächst wie viele unter den Gliedern eine gewisse Zahl k nicht übertreffen, wenn k eine bestimmt gewählte Zahl aus der Reihe

$$0,\ 1,\ 2,\ \ldots,\ \frac{a-1}{2}$$

bedeutet.

Nehmen wir an, dass das letzte unter denjenigen Gliedern der Reihe

$$(18)\quad E\frac{a}{p},\ E\frac{2a}{p},\ \ldots,\ E\frac{la}{p},\ E\frac{(l+1)a}{p},\ \ldots,\ E\frac{\frac{1}{2}(p-1)a}{p},$$

welche die Zahl k nicht übertreffen, das Glied $E\frac{la}{p}$ sei, so wird dieses offenbar dann stattfinden, wenn

$$\frac{la}{p} < k+1 \text{ und } \frac{(l+1)a}{p} > k+1$$

sein wird*).

Aus diesen Ungleichungen ergeben sich die folgenden

$$\frac{p(k+1)}{a} - l > 0 \quad \text{und} \quad \frac{p(k+1)}{a} - l < 1,$$

woraus ersichtlich ist, dass $\frac{p(k+1)}{a}$ um einen positiven echten Bruch grösser als die ganze Zahl l ist. Folglich ist l die grösste in $\frac{p(k+1)}{a}$ enthaltene ganze Zahl, was nach unserer Bezeichnung so dargestellt wird:

$$l = E\frac{p(k+1)}{a}.$$

Wir ersehen also, dass die Anzahl derjenigen Glieder der

---

*) Gleichheit kann offenbar hier nicht stattfinden, weil die Brüche

$$\frac{a}{p},\ \frac{2a}{p},\ \ldots,\ \frac{\frac{1}{2}(p-1)a}{p},$$

in denen p eine Primzahl und kein Theiler von a ist, keiner ganzen Zahl gleich sein können; die Brüche $\frac{la}{p}$, $\frac{(l+1)a}{p}$ sind aber aus der ebenangeführten Reihe entnommen.

Reihe (18), welche die ganze Zahl k nicht übertreffen, genau

$$E\frac{p(k+1)}{a}$$

beträgt.

In derselben Weise findet man, dass hierbei die Anzahl derjenigen Glieder, welche die Zahl $k-1$ nicht übertreffen, $E\frac{pk}{a}$ beträgt; woraus wir dann schliessen, dass die Anzahl derjenigen Glieder, welche genau den Werth k haben, durch die Differenz

$$E\frac{p(k+1)}{a} - E\frac{pk}{a}$$

sich ausdrücken lässt.

In der Reihe (18) befinden sich somit

$E\frac{p}{a} - E\frac{0 \cdot p}{a}$	Glieder,	deren	Werth	0	ist,
$E\frac{2p}{a} - E\frac{p}{a}$	"	"	"	1	",
$E\frac{3p}{a} - E\frac{2p}{a}$	"	"	"	2	",
. . . . .	. . .	. . .	. . .	. . .	. . .
$E\frac{\frac{1}{2}(a-1)p}{a} - E\frac{\frac{1}{2}(a-3)p}{a}$	"	"	"	$\frac{a-1}{2}-1$	".

Was nun die Anzahl aller übrigen Glieder der Reihe (18) betrifft, welche alle den Werth $\frac{a-1}{2}$ haben, so finden wir dieselbe, indem wir die vorhergehenden Zahlen addiren und ihre Summe

$$E\frac{\frac{1}{2}(a-1)p}{a}$$

von der Anzahl aller Glieder der Reihe (18) überhaupt, d. h. von $\frac{1}{2}(p-1)$ subtrahiren. Es ist somit die Anzahl derjenigen Glieder, welche den Werth $\frac{a-1}{2}$ besitzen, durch die Differenz

$$\frac{p-1}{2} - E\frac{\frac{1}{2}(a-1)p}{a}$$

ausgedrückt.

Man kann somit die Summe aller Glieder der Reihe (18) in der Form

$$0 \,.\left(E\frac{p}{a} - E\frac{0\,.\,p}{a}\right) + 1\,.\left(E\frac{2p}{a} - E\frac{p}{a}\right) + 2\,.\left(E\frac{3p}{a} - E\frac{2p}{a}\right) + \ldots +$$

$$+\left(\frac{a-1}{2}-1\right)\left(E\frac{\frac{1}{2}(a-1)p}{a} - E\frac{\frac{1}{2}(a-3)p}{a}\right) + \frac{a-1}{2}\left(\frac{p-1}{2} - E\frac{\frac{1}{2}(a-1)p}{a}\right)$$

darstellen, welche sich auch auf die Form

$$\frac{a-1}{2}\cdot\frac{p-1}{2} - E\frac{p}{a} - E\frac{2p}{a} - \ldots - E\frac{\frac{1}{2}(a-1)p}{a}$$

bringen lässt.

Es ist somit die Summe

$$E\frac{a}{p} + E\frac{2a}{p} + \ldots + E\frac{\frac{1}{2}(p-1)a}{p}$$

der Summe

$$\frac{a-1}{2}\cdot\frac{p-1}{2} - E\frac{p}{a} - E\frac{2p}{a} - \ldots - E\frac{\frac{1}{2}(a-1)p}{a}$$

gleich. Aus dieser Gleichung, in Verbindung mit der im Zusatz I zu Lehrsatz 31 für jede ungerade Zahl a, welche kein Vielfaches der Primzahl p ist, bewiesenen Gleichung (17):

$$\left(\frac{a}{p}\right) = (-1)^{E\frac{a}{p} + E\frac{2a}{p} + \ldots + E\frac{\frac{1}{2}(p-1)a}{p}},$$

erhält man folglich die für dasselbe Symbol $\left(\frac{a}{p}\right)$, unter der Bedingung $a < p$ gültige Gleichung:

$$\left(\frac{a}{p}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{p-1}{2} - E\frac{p}{a} - E\frac{2p}{a} - \ldots - E\frac{\frac{1}{2}(a-1)p}{a}},$$

was wir beweisen wollten.

Auch dieser Lehrsatz kann dazu dienen, den Werth von $\left(\frac{a}{p}\right)$ zu berechnen, wenn a ungerade und kleiner als p ist. Diese Berechnung ist sehr bequem, wenn a keine grosse Zahl ist.

Beispiel. Wir erhalten für $\left(\frac{7}{101}\right)$ den Werth

$$\left(\frac{7}{101}\right) = (-1)^{\frac{7-1}{2}\cdot\frac{101-1}{2} - E\frac{101}{7} - E\frac{2.101}{7} - E\frac{3.101}{7}};$$

woraus sich sofort ergiebt:

$$\left(\frac{7}{101}\right) = (-1)^{3.50-14-28-43} = -1.$$

Besonders bemerkenswerth ist aber dieser Lehrsatz darum, weil aus ihm in sehr einfacher Weise folgender unter dem Namen des *Reciprocitätsgesetzes zweier Primzahlen* bekannter Lehrsatz von Legendre hergeleitet werden kann.

34. *Lehrsatz. Sind v und s ungerade und von einander verschiedene Primzahlen, so ist*

$$\left(\frac{v}{s}\right) = \left(\frac{s}{v}\right)(-1)^{\frac{v-1}{2}\cdot\frac{s-1}{2}}.$$

Beweis. Mag v die kleinere von den beiden Zahlen v, s sein; nach Lehrsatz 33 gilt, wenn $v < s$ ist, die Gleichung

$$\left(\frac{v}{s}\right) = (-1)^{\frac{v-1}{2}\cdot\frac{s-1}{2} - E\frac{s}{v} - E\frac{2s}{v} - \dots - E\frac{\frac{1}{2}(v-1)s}{v}}.$$

Setzt man aber in Gleichung (17) die Werthe $a = s$; $p = v$, so findet man:

$$\left(\frac{s}{v}\right) = (-1)^{E\frac{s}{v} + E\frac{2s}{v} + \dots + E\frac{\frac{1}{2}(v-1)s}{v}},$$

Multiplicirt man diese beiden Gleichungen gliedweise miteinander, so erhält man

$$\left(\frac{v}{s}\right)\left(\frac{s}{v}\right) = (-1)^{\frac{v-1}{2}\cdot\frac{s-1}{2}}.$$

Multiplicirt man ferner beide Seiten der letzten Gleichung mit $\left(\frac{s}{v}\right)$ und berücksichtigt, dass $\left(\frac{s}{v}\right)^2 = 1$ ist, so erhält man:

$$\left(\frac{v}{s}\right) = \left(\frac{s}{v}\right) (-1)^{\frac{v-1}{2} \cdot \frac{s-1}{2}},$$

was zu beweisen war.

Beipiele. 1) Man erhält leicht:

$$\left(\frac{5}{7}\right) = \left(\frac{7}{5}\right) (-1)^{\frac{7-1}{2} \cdot \frac{5-1}{2}} = \left(\frac{7}{5}\right) (-1)^{3 \cdot 2} = \left(\frac{7}{5}\right).$$

2) Dagegen ist

$$\left(\frac{11}{19}\right) = \left(\frac{19}{11}\right) (-1)^{\frac{11-1}{2} \cdot \frac{19-1}{2}} = \left(\frac{19}{11}\right) (-1)^{5 \cdot 9} = -\left(\frac{19}{11}\right).$$

---

§ 27. **Methode, um in allen Fällen den Werth des Symbols $\left(\frac{q}{p}\right)$ zu finden.**

Auf Grund der bis jetzt in Bezug auf $\left(\frac{q}{p}\right)$ bewiesenen Lehrsätze ist es nun leicht seinen Werth zu berechnen, wie gross auch die Zahlen p und q sein mögen.

Man verfahre bei der Auswerthung von $\left(\frac{q}{p}\right)$ wie folgt:

1) Ist q grösser als p, so ersetze man in $\left(\frac{q}{p}\right)$ die Zahl q, nach Lehrsatz 30, durch den Rest der Division von q durch p; oder auch durch den kleinsten negativen Rest von q in Bezug auf Modul p, falls dieser Rest bedeutend kleiner als der erstere ist.

2) Auf diese Weise hat man die Bestimmung des Werthes von $\left(\frac{q}{p}\right)$ auf diejenige von $\left(\frac{\pm R}{p}\right)$ zurückgeführt, wobei R jedenfalls kleiner als p ist. Was nun das Vorzeichen $(-)$ von R betrifft, so kann man, nach Lehrsatz 29, die Untersuchung von $\left(\frac{-R}{p}\right)$ auf die von $\left(\frac{R}{p}\right)$ zurückführen.

3) Um dann $\left(\frac{R}{p}\right)$ zu berechnen, zerlegen wir R in seine Primzahlfactoren, indem wir Factoren, welche ein vollständiges Quadrat bilden, vernachlässigen.

4) Haben wir R als Product von lauter Primzahlfactoren dargestellt, so erhalten wir nach Lehrsatz 29 für $\left(\frac{R}{p}\right)$ ein Product von lauter Factoren der Form $\left(\frac{r}{p}\right)$, wobei r eine Primzahl bedeutet.

5) Darauf verfahren wir bei der Berechnung dieser einzelnen Factoren folgendermassen. Ist $r = 2$, so bestimmt sich der Werth von $\left(\frac{r}{p}\right)$ nach Lehrsatz 31, Zusatz II u. 32. Ist r ungerade, so drücken wir $\left(\frac{r}{p}\right)$ nach dem Reciprocitätsgesetz durch $\left(\frac{p}{r}\right)$ aus und verfahren dann mit $\left(\frac{p}{r}\right)$ genau ebenso, wie wir früher mit $\left(\frac{q}{p}\right)$ verfuhren und so wird die Untersuchung auf die von $\left(\frac{r'}{r}\right)$ zurückgeführt, wobei $r' < r$.

6) Indem wir in derselben Weise fortfahren, erhalten wir Symbole mit immer kleineren und kleineren Zahlen und kommen nothwendigerweise schliesslich entweder auf $\left(\frac{1}{r_n}\right)$, oder auf $\left(\frac{2}{r_n}\right)$, deren Werth wir leicht finden können, um dadurch auch den gesuchten Werth von $\left(\frac{q}{p}\right)$ zu bestimmen.

Beispiele. 1. Es werde der Werth von $\left(\frac{1013}{601}\right)$ gesucht. Indem wir 1013 durch 601 dividiren, finden wir 412 als Rest; folglich ist $\left(\frac{1013}{601}\right) = \left(\frac{412}{601}\right)$.

Es ist nun $412 = 2^2 . 103$ und weil wir das Quadrat von 2 vernachlässigen können, so wird $\left(\frac{412}{601}\right) = \left(\frac{103}{601}\right)$.

Nach dem Reciprocitätsgesetze ist aber

$$\left(\frac{103}{601}\right) = \left(\frac{601}{103}\right) (-1)^{\frac{103-1}{2} \cdot \frac{601-1}{2}} = \left(\frac{601}{103}\right).$$

Dividiren wir darauf 601 durch 103, so finden wir 86 als Rest; dagegen ergiebt sich als kleinster negativer Rest von 601 in Bezug auf den Modul 103 die bedeutend kleinere Zahl —17 und wir finden es bequemer diese letztere zu gebrauchen[*)]. Man betrachte also

$$\left(\frac{601}{103}\right) = \left(\frac{-17}{103}\right).$$

Da aber

$$\left(\frac{-17}{103}\right) = \left(\frac{-1}{103}\right)\left(\frac{17}{103}\right) \text{ und } \left(\frac{-1}{103}\right) = (-1)^{\frac{103-1}{2}} = -1$$

ist, so erhalten wir

$$\left(\frac{-17}{103}\right) = -\left(\frac{17}{103}\right).$$

Weil 17 eine ungerade Primzahl ist, so können wir wiederum das Reciprocitätsgesetz anwenden und finden

$$\left(\frac{17}{103}\right) = \left(\frac{103}{17}\right)(-1)^{\frac{103-1}{2}\cdot\frac{17-1}{2}} = \left(\frac{103}{17}\right).$$

Ersetzen wir in $\left(\frac{103}{17}\right)$ die Zahl 103 durch ihren kleinsten positiven Rest in Bezug auf den Modul 17, welcher hier 1 ist, so erhalten wir

$$\left(\frac{103}{17}\right) = \left(\frac{1}{17}\right) = 1.$$

Die Verbindung aller dieser Gleichungen ergiebt schliesslich:

[*)] Uebrigens würde der Rest 86 in folgender Weise zum Ziele führen. Es ist zunächst:

$$\left(\frac{86}{103}\right) = \left(\frac{2}{103}\right)\left(\frac{43}{103}\right).$$

Nun ist

$$\left(\frac{2}{103}\right) = 1$$

und

$$\left(\frac{43}{103}\right)=\left(\frac{103}{43}\right)(-1)^{21.51}=-\left(\frac{103}{43}\right)=-\left(\frac{17}{43}\right)=-\left(\frac{43}{17}\right)=-\left(\frac{9}{17}\right)=-1.]$$

$$\left(\frac{1013}{601}\right) = \left(\frac{412}{601}\right) = \left(\frac{601}{103}\right) = \left(\frac{-17}{103}\right) = -\left(\frac{17}{103}\right) =$$

$$-\left(\frac{103}{17}\right) = -\left(\frac{1}{17}\right) = -1.$$

Es ist also in unserem Beispiele

$$\left(\frac{1013}{601}\right) = -1.$$

2. Der Werth von $\left(\frac{20470}{1847}\right)$ wird gesucht. Indem wir berücksichtigen, dass als kleinster positiver Rest von 20470 in Bezug auf den Modul 1847 sich $153 = 3^2 . 17$ ergiebt, so erhalten wir

$$\left(\frac{20470}{1847}\right) = \left(\frac{153}{1847}\right) = \left(\frac{3^2 . 17}{1847}\right) = \left(\frac{17}{1847}\right).$$

Dann ist

$$\left(\frac{17}{1847}\right) = \left(\frac{1847}{17}\right)(-1)^{\frac{17-1}{2} \cdot \frac{1847-1}{2}} = \left(\frac{1847}{17}\right) = \left(\frac{11}{17}\right),$$

und

$$\left(\frac{11}{17}\right) = \left(\frac{17}{11}\right)(-1)^{\frac{17-1}{2} \cdot \frac{11-1}{2}} = \left(\frac{17}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right).$$

Es ist aber $\left(\frac{2}{11}\right) = -1$ und

$$\left(\frac{3}{11}\right) = \left(\frac{11}{3}\right)(-1)^{\frac{11-1}{2} \cdot \frac{3-1}{2}} = -\left(\frac{11}{3}\right) = -\left(\frac{-1}{3}\right) = 1.$$

Die Verbindung aller dieser Gleichungen ergiebt also

$$\left(\frac{20470}{1847}\right) = -1.$$

3. Es soll der Werth von $\left(\frac{2108}{2003}\right)$ berechnet werden. Man findet zunächst:

$$\left(\frac{2108}{2003}\right) = \left(\frac{105}{2003}\right) = \left(\frac{3}{2003}\right)\left(\frac{5}{2003}\right)\left(\frac{7}{2003}\right).$$

Ferner:

$$\left(\frac{3}{2003}\right)=\left(\frac{2003}{3}\right)(-1)^{\frac{3-1}{2}\cdot\frac{2003-1}{2}}=-\left(\frac{2003}{3}\right)=-\left(\frac{2}{3}\right)=1;$$

$$\left(\frac{5}{2003}\right)=\left(\frac{2003}{5}\right)(-1)^{\frac{5-1}{2}\cdot\frac{2003-1}{2}}=\left(\frac{2003}{5}\right)=\left(\frac{3}{5}\right)=$$

$$\left(\frac{5}{3}\right)(-1)^{2.1}=\left(\frac{5}{3}\right)=\left(\frac{2}{3}\right)=-1;$$

$$\left(\frac{7}{2003}\right)=\left(\frac{2003}{7}\right)(-1)^{\frac{7-1}{2}\cdot\frac{2003-1}{2}}=-\left(\frac{2003}{7}\right)=$$

$$-\left(\frac{1}{7}\right)=-1;$$

und somit ist

$$\left(\frac{2108}{2003}\right)=1.$$

---

§ 28. Lösung der Gleichungen $\left(\frac{x}{p}\right)=1;\quad \left(\frac{x}{p}\right)=-1.$

Wir haben gezeigt, wie man, wenn q und p gegeben sind, den Werth des Legendre'schen Symbols $\left(\frac{q}{p}\right)$ berechnen kann, um dadurch zu entscheiden ob eine Congruenz

$$z^2 \equiv q \pmod{p}$$

Lösungen hat, oder nicht. Wir gehen jetzt zur Lösung der umgekehrten Aufgabe über:

Der Werth des Symbols $\left(\frac{x}{p}\right)$ sei gegeben, der Werth von x soll gefunden werden.

Mit anderen Worten:

es wird die Lösung der Gleichungen

$$\left(\frac{x}{p}\right) = 1; \quad \left(\frac{x}{p}\right) = -1$$

gesucht.

Wir beginnen mit der ersteren Gleichung $\left(\frac{x}{p}\right) = 1$. Wie wir gesehen haben, drückt die Gleichung $\left(\frac{x}{p}\right) = 1$ nichts anderes aus, als dass die Congruenz

$$x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

befriedigt werden kann.

Es ist nicht schwer zu erkennen, dass diese Congruenz $\frac{p-1}{2}$ Lösungen hat. Zu diesem Zwecke dividiren wir, nach § 21, den Ausdruck $x^p - x$ durch $x^{\frac{p-1}{2}} - 1$ und indem wir bemerken, dass

$$x^p - x = x\left(x^{\frac{p-1}{2}} + 1\right)\left(x^{\frac{p-1}{2}} - 1\right)$$

durch $x^{\frac{p-1}{2}} - 1$ ohne Rest theilbar ist, so schliessen wir, nach Lehrsatz 26, dass die Congruenz

$$x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

$\frac{p-1}{2}$ Lösungen besitzt.

Diese Lösungen werden aber (nach § 12) durch

$$x \equiv a_1, \quad x \equiv a_2, \quad \ldots\ldots, \quad x \equiv a_{\frac{p-1}{2}} \pmod{p}$$

dargestellt, wobei

$$a_1, \quad a_2, \quad \ldots\ldots, \quad a_{\frac{p-1}{2}}$$

diejenigen Zahlen aus der Reihe

$$0, 1, 2, \ldots, p-1$$

sind, welche die Congruenz

$$x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

befriedigen.

Es ist aber klar, dass keine dieser Zahlen der Null gleich sein kann, weil die Null nicht die Congruenz

$$x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

befriedigen kann. Folglich befinden sich in der Reihe

$$1, 2, \ldots, p-1$$

$\frac{p-1}{2}$ Zahlen, welche die Congruenz $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, also auch die Gleichung $\left(\frac{x}{p}\right) = 1$ befriedigen. Mit anderen Worten: unter den Zahlen der Reihe

$$1, 2, \ldots, p-1$$

sind $\frac{p-1}{2}$ solche vorhanden, welche *quadratische Reste* nach dem Modul p sind. Dann müssen aber alle übrigen Zahlen dieser Reihe, deren Anzahl ebenfalls $\frac{p-1}{2}$ sein wird, die Gleichung

$$\left(\frac{x}{p}\right) = -1$$

befriedigen; dieselben sind *quadratische Nichtreste* nach dem Modul p.

Aus dieser Auseinandersetzung ergiebt sich, dass alle Zahlen überhaupt, welche der Congruenz $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, also auch der Gleichung $\left(\frac{x}{p}\right) = 1$ genügen, durch die Congruenzen

$$x \equiv a_1, \quad x \equiv a_2, \quad \ldots, \quad x \equiv a_{\frac{p-1}{2}} \pmod{p}$$

bestimmt sind, wobei

$$a_1, \; a_2, \; \ldots, \; a_{\frac{p-1}{2}}$$

positive Zahlen bedeuten, welche kleiner als p sind und die Congruenz $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ befriedigen.

Wir würden diese Zahlen dadurch finden können, dass wir die Lösungen der letzgenannten Congruenz wirklich aufsuchen. Dieses Verfahren würde aber ausserordentlich beschwerlich werden, wenn p eine grosse Zahl ist. Daher wollen wir ein anderes Verfahren zeigen, wie man die gesuchten Zahlen unabhängig von der Lösung der Congruenz $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ finden kann. Zu diesem Zwecke erinnern wir uns, dass die Congruenz $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ die Bedingung für die Möglichkeit der Congruenz

$$z^2 \equiv a \pmod{p}$$

war.

Von dieser letzteren Congruenz haben wir (§ 22) gesehen, dass dieselbe, wenn sie überhaupt möglich ist, durch zwei Zahlen aus der Reihe $1, 2, \ldots, p-1$ befriedigt wird, und zwar so dass, wenn die eine der zwei Zahlen α ist, die andere $p-\alpha$ wird. Da aber *eine* von den zwei Zahlen nothwendigerweise kleiner als $\frac{p}{2}$ ist, so können sie auch nicht beide grösser als $\frac{p-1}{2}$ sein; weil die Summe beider Zahlen p ist, während sie von einander verschieden sind.

Befriedigt daher eine Zahl a die Congruenz $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, so wird man immer in der Reihe

$$1, 2, \ldots, \frac{p-1}{2}$$

eine Zahl finden, welche, für z gesetzt, die Congruenz

$$z^2 \equiv a \pmod{p}$$

befriedigt. Mit anderen Worten: für eine solche Zahl a wird immer *eine* der Congruenzen

$$1^2 \equiv a, \quad 2^2 \equiv a, \quad \ldots, \quad \left(\frac{p-1}{2}\right)^2 \equiv a \pmod{p}$$

stattfinden. Es muss also a in Bezug auf den Modul p einer der Zahlen

$$1^2,\ 2^2,\ \ldots,\ \left(\frac{p-1}{2}\right)^2$$

congruent sein; weil nun a kleiner als p sein soll, so muss man a unter den Resten der Division dieser Zahlen durch p finden.

Jede der $\frac{p-1}{2}$ Zahlen

$$a_1,\ a_2,\ \ldots,\ a_{\frac{p-1}{2}},$$

welche kleiner als p sind und die Congruenz

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

befriedigen, finden wir daher unter der Reihe der $\frac{p-1}{2}$ Reste, welche nach der Division der $\frac{p-1}{2}$ Zahlen

$$1^2,\ 2^2,\ \ldots,\ \left(\frac{p-1}{2}\right)^2$$

durch p sich ergeben.

Darauf wird der Werth von x, welcher die Gleichung

$$\left(\frac{x}{p}\right) = 1$$

befriedigen soll, durch die Congruenzen

$$x \equiv a_1,\ x \equiv a_2,\ \ldots,\ x \equiv a_{\frac{p-1}{2}} \pmod{p}$$

bestimmt.

Wir erhalten somit (nach § 11, indem wir dort in den Formeln die Zahl N durch $-n$ ersetzen) die Lösungen der Gleichung

$$\left(\frac{x}{p}\right) = 1$$

in der Form

$$x = np + a_1;\ x = np + a_2,\ \ldots,\ x = np + a_{\frac{p-1}{2}}$$

dargestellt.

Beispiel. Es werden die Lösungen der Gleichung

$$\left(\frac{x}{11}\right) = 1$$

gesucht.

Diese Gleichung wird nach der obigen Auseinandersetzung

$$\frac{11-1}{2} = 5$$

Lösungen haben, welche durch die Congruenzen

$$x \equiv a_1,\ x \equiv a_2,\ x \equiv a_3,\ x \equiv a_4,\ x \equiv a_5 \pmod{11}$$

sich darstellen lassen, wenn

$$a_1,\ a_2,\ a_3,\ a_4,\ a_5$$

die Reste sind, welche bei der Division der Zahlen

$$1^2,\ 2^2,\ 3^2,\ 4^2,\ 5^2,$$

durch 11 sich ergeben. Da nun diese Reste die Zahlen

$$1,\ 4,\ 9,\ 5,\ 3$$

sind, so erhält man die Lösungen der Gleichung

$$\left(\frac{x}{11}\right) = 1$$

in der Form

$$x \equiv 1,\ x \equiv 3,\ x \equiv 4,\ x \equiv 5,\ x \equiv 9 \pmod{11},$$

oder, was dasselbe ist, die Lösungen sind durch die Formeln

$$x = 11n + 1,\ x = 11n + 3,\ x = 11n + 4,\ x = 11n + 5,$$
$$x = 11n + 9$$

dargestellt.

Kennt man nun die Lösungen der Gleichung $\left(\frac{x}{p}\right) = 1$, so sind die Lösungen von $\left(\frac{x}{p}\right) = -1$ leicht zu finden.

Wir bemerken zu diesem Zwecke, *erstens* dass bei der Bedeutung des Symbols $\left(\frac{x}{p}\right)$ vorausgesetzt war, dass x nicht durch p theilbar sei; und *zweitens*, dass diejenigen Zahlen, welche der Gleichung $\left(\frac{x}{p}\right) = 1$ nicht genügen, nothwendigerweise die Gleichung $\left(\frac{x}{p}\right) = -1$ befriedigen. Daraus folgt, dass wir alle Zahlen, für welche die Gleichung $\left(\frac{x}{p}\right) = -1$ stattfindet, dadurch erhalten, dass wir von allen den Zahlen, welche durch p nicht theilbar sind, diejenigen fortlassen, welche die Gleichung $\left(\frac{x}{p}\right) = 1$ befriedigen. Da nun alle Zahlen überhaupt durch die Formen

$$np, \quad np+1, \quad np+2, \quad \ldots, \quad np+p-1$$

dargestellt werden, und da die Zahlen von der Form np, als Vielfache von p, für unseren Zweck ausgeschlossen sind, so bleiben für die Lösungen *beider* Gleichungen $\left(\frac{x}{p}\right) = 1$ und $\left(\frac{x}{p}\right) = -1$ nur noch die Zahlen von den Formen

$$np+1, \quad np+2, \quad \ldots, \quad np+p-1$$

übrig.

Lässt man nun unter diesen die Zahlen von der Form

$$np+a_1, \quad np+a_2, \quad \ldots, \quad np+a_{\frac{p-1}{2}},$$

welche die *eine* jener Gleichungen, nämlich $\left(\frac{x}{p}\right) = 1$ befriedigen, fort, so erhalten wir alle Zahlen, welche die *andere* jener Gleichungen, nämlich $\left(\frac{x}{p}\right) = -1$ befriedigen.

Somit ergiebt sich, dass die Zahlen, welche der Gleichung $\left(\frac{x}{p}\right) = -1$ Genüge leisten, durch die Formen

$$np + b_1,\ np + b_2,\ \ldots,\ np + b_{\frac{p-1}{2}}$$

dargestellt sind, wobei

$$b_1,\ b_2,\ \ldots,\ b_{\frac{p-1}{2}}$$

diejenigen Zahlen aus der Reihe

$$1,\ 2,\ \ldots,\ p-1$$

sind, welche von

$$a_1,\ a_2,\ \ldots,\ a_{\frac{p-1}{2}},$$

d. h. von den Resten der Division von

$$1^2,\ 2^2,\ \ldots,\ \left(\frac{p-1}{2}\right)^2$$

durch p verschieden sind.

Beispiel. Wir suchen die Lösungen von $\left(\frac{x}{11}\right) = -1$. Die Zahlen, die diese Gleichung befriedigen, werden, wie wir gesehen haben, durch die Formen

$$11n + b_1,\ 11n + b_2,\ 11n + b_3,\ 11n + b_4,\ 11n + b_5$$

dargestellt, wobei wir die Zahlen

$$b_1,\ b_2,\ b_3,\ b_4,\ b_5$$

dadurch finden, dass wir in der Reihe

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10$$

diejenigen weglassen, welche als Reste bei der Division von

$$1^2,\ 2^2,\ 3^2,\ 4^2,\ 5^2$$

durch 11 sich ergeben. Solche Reste sind aber die Zahlen

$$1,\ 4,\ 9,\ 5,\ 3;$$

lassen wir diese in der Reihe 1, 2, 3, 4, 5, 6, 7, 8, 9, 10

fort, so bleiben als Werthe von b_1, b_2, b_3, b_4, b_5 die Zahlen

$$2,\ 6,\ 7,\ 8,\ 10.$$

Die Lösungen der Gleichung $\left(\frac{x}{11}\right) = -1$ ergeben sich somit durch die Formen

$$11n+2,\quad 11n+6,\quad 11n+7,\quad 11n+8,\quad 11n+10.$$

In dieser Weise wird somit die Aufgabe über die Bestimmung von x, wenn $\left(\frac{x}{p}\right)$ gegeben ist, mit anderen Worten, über die Auffindung der *quadratischen Reste* und *Nichtreste* einer gegebenen Zahl gelöst.

---

§ 29. Lösung der Congruenz $z^2 \equiv q \pmod{p}$, wenn p eine Primzahl von der Form $4n+3$ ist.

Wir haben uns in den vorhergehenden Paragraphen mit der Untersuchung beschäftigt, wann die Congruenz $z^2 \equiv q \pmod{p}$ Lösungen hat und wann sie keine hat. Es bleibt uns noch zu zeigen übrig, wie diese Lösungen von $z^2 \equiv q \pmod{p}$ gefunden werden, wenn sie möglich sind.

Später, bei der Behandlung der Congruenzen von der Gestalt

$$a^x \equiv A \pmod{p},$$

werden wir eine allgemeine und sehr einfache Methode für die Lösung der Congruenz $z^2 \equiv q \pmod{p}$ kennen lernen. Hier wollen wir uns mit einem speciellen Falle begnügen, in welchem diese Lösung unmittelbar gefunden werden kann. Dieses ist der Fall, wenn die Primzahl p die Form $4n+3$ hat.

Wir haben oben gesehen, dass die Möglichkeit einer Lösung der Congruenz $z^2 \equiv q \pmod{p}$ voraussetzt, dass

$$q^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

ist. Setzen wir hierin $p = 4n + 3$, so finden wir:

$$q^{\frac{4n+3-1}{2}} \equiv 1 \ (\text{mod.}\, p), \text{ oder } q^{2n+1} \equiv 1 \ (\text{mod.}\, p),$$

welche durch Multiplication beider Seiten mit q in

$$q^{2n+2} \equiv q \ (\text{mod.}\, p)$$

übergeht.

Vergleicht man diese Congruenz mit den vorgelegten $z^2 \equiv q$ (mod. p), so bemerkt man sofort, dass der letzteren die Zahl $z = q^{n+1}$ genügt.

Haben wir nun eine Zahl, welche der Congruenz $z^2 \equiv q$ (mod. p) genügt, gefunden, so ist es leicht deren unendlich viele aus der Congruenz $z^2 \equiv q^{n+1}$ (mod. p) zu finden. Wir haben aber gesehen, dass eine von diesen Zahlen positiv und kleiner als p sein wird; es ist dieses nämlich der Rest bei der Division von q^{n+1} durch p. Bezeichnen wir diesen Rest mit α, so wird eine der beiden Lösungen der Congruenz $z^2 \equiv q$ (mod. p) durch $z \equiv \alpha$ (mod. p) dargestellt sein. Was nun die zweite Lösung betrifft, so wird dieselbe, nach § 22, durch $z \equiv p - \alpha$ (mod. p) dargestellt.

Somit haben wir beide Lösungen der Congruenz $z^2 \equiv q$ (mod. p) gefunden, wenn $p = 4n + 3$ ist.

Beispiel. Es sollen die Lösungen von

$$z^2 \equiv 3 \ (\text{mod.}\, 11)$$

gefunden werden.

Diese Congruenz ist möglich, weil

$$\left(\frac{3}{11}\right) = \left(\frac{11}{3}\right)(-1)^{\frac{11-1}{2}\cdot\frac{3-1}{2}} = -\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = 1;$$

da aber $11 = 4.2 + 3$ ist, so werden die Lösungen unserer Congruenz

$$z \equiv \alpha \text{ und } z \equiv 11 - \alpha \ (\text{mod.}\, 11)$$

sein, wobei α der Rest der Division von 3^{2+1} durch 11, also $\alpha = 5$ ist. Die beiden Lösungen der Congruenz

$$z^2 \equiv 3 \pmod{11}$$

sind somit:

$$z \equiv 5 \text{ und } z \equiv 6 \pmod{11}.$$

---

§ 30. Ueber die Congruenz $z^2 \equiv q \pmod{p}$, wenn p eine zusammengesetzte Zahl ist.

Bis jetzt haben wir uns ausschliesslich mit der Untersuchung solcher Congruenzen zweiten Grades beschäftigt, deren Modul eine Primzahl ist. Was nun solche Congruenzen betrifft, deren Modul eine zusammengesetzte Zahl ist, so wollen wir uns auf den Beweis beschränken, dass

eine Congruenz $z^2 \equiv q \pmod{p}$ eine Lösung hat, wenn p ungerade und relativ prim zu q ist und aus den Primzahlen

$$\alpha, \beta, \gamma, \ldots.$$

zusammengesetzt, für welche die Gleichungen

$$\left(\frac{q}{\alpha}\right) = 1, \quad \left(\frac{q}{\beta}\right) = 1, \quad \left(\frac{q}{\gamma}\right) = 1, \ldots.$$

stattfinden.

Wir beginnen mit dem speciellen Falle $p = \alpha^m$ und wollen zeigen, wie man die Lösungen der Congruenz

$$z^2 \equiv q \pmod{\alpha^m}$$

finden kann, wenn die Lösungen von

$$z^2 \equiv q \pmod{\alpha}$$

bekannt sind, deren Möglichkeit, wie wir wissen, durch die Gleichung

$$\left(\frac{q}{\alpha}\right) = 1$$

bedingt ist.

Nehmen wir an, es sei a eine Zahl, welche die Congruenz $z^2 \equiv q \pmod{\alpha}$ befriedigt und P, Q seien durch die Gleichungen

$$P = \frac{(a+\sqrt{q})^m + (a-\sqrt{q})^m}{2}$$

$$Q = \frac{(a+\sqrt{q})^m - (a-\sqrt{q})^m}{2\sqrt{q}}$$

definirt. Man kann sich leicht, durch Entwickelung von $(a+\sqrt{q})^m$ und $(a-\sqrt{q})^m$ nach dem binomischen Lehrsatze, überzeugen, dass P und Q ganze Zahlen sind[*)]. Wir wollen nun beweisen, dass

1) *P und Q die Congruenz*

$$P^2 - Q^2 q \equiv 0 \pmod{\alpha^m}$$

befriedigen;

2) *Q ist relativ prim zu α.*

Von der Richtigkeit der ersteren Behauptung überzeugen wir uns leicht, indem wir bemerken, dass aus den obigen Gleichungen sich die Beziehungen

---

[*) Um hier nichts unbewiesenes vorauszusetzen, wollen wir den leicht zu führenden Beweis hinzufügen.

Erstens sind die Binomial-Coëfficienten von $(a+b)^k$ bekanntlich immer ganze Zahlen, sobald k eine ganze Zahl ist.

Nimmt man nämlich die Richtigkeit dieser Behauptung für $(a+b)^k$ an, so überzeugt man sich durch Multiplication mit $(a+b)$, dass die Richtigkeit dann auch für $(a+b)^{k+1}$ bestehen bleibt; da nun für $k = 0, 1, 2, 3$ die Behauptung offenbar richtig ist, so muss sie auch für jede ganze positive Zahl k richtig bleiben. (Wir brauchen es hier nur für positive k; indess kann man die Richtigkeit für negative ganze k dadurch beweisen, dass man nur für $(a+b)^{-1}$ beweist).

Zweitens sieht man unmittelbar, dass der Zähler von P bei Vertauschung von $+\sqrt{q}$ und $-\sqrt{q}$ unverändert bleibt, während der Zähler von Q dabei nur das Vorzeichen ändert; es muss daher $\sqrt{q}$ im Zähler von P nur in geraden Potenzen und in demjenigen von Q nur in ungeraden Potenzen auftreten.

Drittens ist der Zähler von Q offenbar durch

$$(a+\sqrt{q}) - (a-\sqrt{q}) = 2\sqrt{q}$$

theilbar; während im Zähler von P alle Coëfficienten der ungeraden Potenzen von $\sqrt{q}$ wegfallen und diejenigen der geraden Potenzen sich verdoppeln, so dass der Zähler von P durch 2 theilbar wird.

Dadurch ist bewiesen, dass P und Q ganze Zahlen sein müssen, **sobald a, q, m solche sind.]**

$$P + Q\sqrt{q} = (a + \sqrt{q})^m, \quad P - Q\sqrt{q} = (a - \sqrt{q})^m$$

ergeben, deren gliedweise Multiplication die Gleichung

$$P^2 - Q^2 q = (a^2 - q)^m$$

liefert.

Nach der Annahme sollte aber a die Congruenz $z^2 \equiv q \pmod{\alpha}$ befriedigen, d. h. es ist $a^2 \equiv q \pmod{\alpha}$, was die Theilbarkeit der Differenz $a^2 - q$ durch α ausdrückt. Hat nun $a^2 - q$ einen Theiler α, so muss

$$P^2 - Q^2 q = (a^2 - q)^m$$

den Theiler α^m besitzen, d. h. es findet die Congruenz

$$P^2 - Q^2 q \equiv 0 \pmod{\alpha^m}$$

statt.

Nachdem wir die Richtigkeit der ersten Behauptung bewiesen haben, gehen wir zum Beweise der zweiten Behauptung über, dass nämlich Q relativ prim zu a ist.

Zu diesem Ende bemerken wir, dass nach der Gleichung

$$Q = \frac{(a + \sqrt{q})^m - (a - \sqrt{q})^m}{2\sqrt{q}}$$

die Theilbarkeit von Q durch α die Bestehung der Congruenz

$$\frac{(a + \sqrt{q})^m - (a - \sqrt{q})^m}{2\sqrt{q}} \equiv 0 \pmod{\alpha} \quad . \quad . \quad . \quad (\lambda)$$

aussagen würde. Die linke Seite dieser Congruenz enthält q, wie man sich leicht durch Entwicklung der Ausdrücke

$$(a + \sqrt{q})^m; \quad (a - \sqrt{q})^m$$

überzeugen kann, nur in ganzen positiven Potenzen und mit ganzzahligen Coëfficienten. Die Congruenz würde somit (nach § 10, Lehrsatz 13) auch noch richtig bleiben, wenn wir darin q durch a^2 ersetzen, weil $a^2 \equiv q \pmod{\alpha}$ ist. Folglich würde die Congruenz (λ) in

$$\frac{(a + \sqrt{a^2})^m - (a - \sqrt{a^2})^m}{2\sqrt{a^2}} \equiv 0 \pmod{\alpha}$$

übergehen, welche auf

$$2^{m-1}\ a^{m-1} \equiv 0 \ (\text{mod. } \alpha)$$

führen würde. Diese Congruenz ist aber unmöglich, weil α eine ungerade Primzahl und a relativ prim zu α war.

Haben wir uns nun überzeugt, dass P, Q die Congruenz

$$P^2 - Q^2 q \equiv 0 \ (\text{mod. } \alpha^m)$$

befriedigen und, dass Q relativ prim zu α ist, so wird es leicht sein zu beweisen:

1) *Die Congruenz* $Qx \equiv P$ (mod. α^m) *besitzt eine Lösung*;

2) *Diese Lösung befriedigt die Congruenz*

$$x^2 \equiv q \ (\text{mod. } \alpha^m).$$

Erstere Behauptung folgt direct aus dem Umstande, dass Q relativ prim zu α und somit auch zu α^m ist; in diesem Falle hat aber die Congruenz $Qx - P \equiv 0$ (mod. α^m) (nach § 13, Lehrsatz 15) immer eine Lösung.

Es bleibt uns also nur noch zu beweisen, dass die Zahlen x, welche die Congruenz

$$Qx \equiv P \ (\text{mod. } \alpha^m)$$

befriedigen, zugleich auch, für z gesetzt, der Congruenz

$$z^2 \equiv q \ (\text{mod. } \alpha^m)$$

Genüge leisten. Zu diesem Ende erheben wir beide Seiten der ersteren Congruenz zum Quadrat und erhalten

$$Q^2 x^2 \equiv P^2 \ (\text{mod. } \alpha^m).$$

Verbinden wir diese Congruenz mit der oben bewiesenen

$$P^2 - Q^2 q \equiv 0 \ (\text{mod. } \alpha^m),$$

so erhalten wir

$$Q^2 x^2 \equiv Q^2 q \ (\text{mod. } \alpha^m),$$

deren beide Seiten durch Q^2 dividirt werden dürfen, weil Q relativ prim zu α, also auch zu α^m ist. Wir erhalten also

$$x^2 \equiv q \pmod{\alpha^m},$$

was zu beweisen war.

Wir finden somit die Lösungen von

$$z^2 \equiv q \pmod{\alpha^m}$$

aus der Congruenz

$$Qz \equiv P \pmod{\alpha^m},$$

wobei P, Q aus den Gleichungen

$$P = \frac{(a+\sqrt{q})^m + (a-\sqrt{q})^m}{2}; \quad Q = \frac{(a+\sqrt{q})^m - (a-\sqrt{q})^m}{2\sqrt{q}}$$

gefunden werden, wenn a eine Zahl bedeutet, welche die Congruenz

$$a^2 \equiv q \pmod{\alpha}$$

befriedigt.

Beispiel. Es sollen die Lösungen der Congruenz

$$z^2 \equiv -2 \pmod{3^3}$$

gefunden werden.

Man findet, nach der obigen Auseinandersetzung, eine diese Congruenz befriedigende Zahl aus der Congruenz

$$Qz \equiv P \pmod{3^3},$$

wobei

$$P = \frac{(a+\sqrt{-2})^3 + (a-\sqrt{-2})^3}{2};$$

$$Q = \frac{(a+\sqrt{-2})^3 - (a-\sqrt{-2})^3}{2\sqrt{-2}},$$

wenn a die Congruenz

$$a^2 \equiv -2 \pmod{3}$$

befriedigt.

Die letzte Congruenz gehört zu denjenigen, welche nach der im § 29 gezeigten Methode gelöst werden können. Wir finden nach dieser Methode, dass die Zahl $a = 1$ die Congruenz befriedigt, wovon man sich im gegebenen Falle auch unmittelbar überzeugt. Setzt man diesen Werth $a = 1$ in die obigen, P, Q definirenden Gleichungen ein, so erhält man:

$$P = \frac{(1+\sqrt{-2})^3 + (1-\sqrt{-2})^3}{2} = -5$$

$$Q = \frac{(1+\sqrt{-2})^3 - (1-\sqrt{-2})^3}{2\sqrt{-2}} = 1.$$

Daraus ergiebt sich eine Zahl z, welche die Congruenz

$$z^2 \equiv -2 \pmod{3^3}$$

befriedigt, in der Form

$$z \equiv -5 \pmod{3^3}.$$

Nachdem wir gezeigt haben, wie die Lösungen einer Congruenz $z^2 \equiv q \pmod{\alpha^m}$, wenn α irgend eine ungerade Primzahl ist, gefunden werden, können wir leicht zur Lösung der allgemeinern Congruenz

$$z^2 \equiv q \pmod{\alpha^m\ \beta^n\ \gamma^r\ \dots}$$

übergehen.

Hat man gleichzeitig

$$\left(\frac{q}{\alpha}\right) = 1;\quad \left(\frac{q}{\beta}\right) = 1;\quad \left(\frac{q}{\gamma}\right) = 1;\ \dots,$$

so findet man nach der eben angegebenen Methode solche Zahlen $u, v, w, \dots$, welche die Congruenzen

$$u^2 \equiv q \pmod{\alpha^m};\quad v^2 \equiv q \pmod{\beta^n};\quad w^2 \equiv q \pmod{\gamma^r};\ \dots$$

befriedigen. Diese Zahlen werden, wie wir gesehen haben, durch Congruenzen von der Gestalt

$$u \equiv A \pmod{\alpha^m};\quad v \equiv B \pmod{\beta^n};\quad w \equiv C \pmod{\gamma^r};\ \dots$$

dargestellt.

Man kann sich aber leicht überzeugen, dass unter den Zahlen, welche durch jede dieser Congruenzen definirt sind, sich eine Zahl x von der Gestalt

$$x = A(\beta^n\gamma^r\dots)^{\alpha^{m-1}(\alpha-1)} + B(\alpha^m\gamma^r\dots)^{\beta^{n-1}(\beta-1)} + C(\alpha^m\beta^n\dots)^{\gamma^{r-1}(\gamma-1)} + \dots$$

finden muss; welche also zugleich alle diese Congruenzen befriedigt.

Denn diese Zahl x, welche aus einer Summe von Gliedern besteht, von denen alle, mit Ausnahme des ersten, Vielfache von α^m sind, genügt offenbar der Congruenz

$$x \equiv A\,(\beta^n \gamma^r \ldots)^{\alpha^{m-1}(\alpha-1)} \pmod{\alpha^m},$$

während nach Lehrsatz 17 die Congruenz

$$(\beta^n \gamma^r \ldots)^{\alpha^{m-1}(\alpha-1)} \equiv 1 \pmod{\alpha^m},$$

also auch

$$A\,(\beta^n \gamma^r \ldots)^{\alpha^{m-1}(\alpha-1)} \equiv A \pmod{\alpha^m}$$

besteht. Man erhält somit für unsere Zahl x die Congruenz

$$x \equiv A \pmod{\alpha^m}.$$

Ebenso kann man beweisen, dass für x die Congruenzen

$$x \equiv B \pmod{\beta^n}$$
$$x \equiv C \pmod{\gamma^r}$$
$$\vdots$$

stattfinden; folglich wird unsere Zahl x die Congruenzen

$$u^2 \equiv q \pmod{\alpha^m}; \quad v^2 \equiv q \pmod{\beta^n}; \quad w^2 \equiv q \pmod{\gamma^r}; \ \ldots.$$

gleichzeitig befriedigen; so dass zugleich die Congruenzen

$$x^2 \equiv q \pmod{\alpha^m}; \quad x^2 \equiv q \pmod{\beta^n}; \quad x^2 \equiv q \pmod{\gamma^r}; \ \ldots.$$

bestehen. Da aber die Moduli

$$\alpha^m, \ \beta^n, \ \gamma^r, \ \ldots$$

dieser Congruenzen relativ prim zu einander sind, weil $\alpha, \beta, \gamma, \ldots$ als von einander verschiedene Primzahlen angenommen waren, so haben die letzten Congruenzen (nach § 9) die Congruenz

$$x^2 \equiv q \ (\text{mod.}\ \alpha^m, \beta^n, \gamma^r, \ldots.)$$

zur Folge.

Auf diese Weise wird eine Zahl x bestimmt, die die Congruenz

$$x^2 \equiv q \pmod{p}$$

befriedigt, wenn q relativ prim zu p und p eine ungerade

Zahl ist, welche aus einem Producte von Potenzen der Primzahlen

$$\alpha, \beta, \gamma, \ldots$$

besteht und die Gleichungen

$$\left(\frac{q}{\alpha}\right) = 1, \quad \left(\frac{q}{\beta}\right) = 1, \quad \left(\frac{q}{\gamma}\right) = 1, \ldots$$

stattfinden.

[*Umkehrung. Besitzt die Congruenz*

$$z^2 - q \equiv 0 \pmod{\alpha^m \beta^n \gamma^r \ldots}$$

eine Lösung, während $\alpha, \beta, \gamma, \ldots$ *von einander und von 2 verschiedene Primzahlen und q relativ prim zu*

$$N = \alpha^m \beta^n \gamma^r \ldots,$$

so bestehen gleichzeitig die Gleichungen

$$\left(\frac{q}{\alpha}\right) = 1; \quad \left(\frac{q}{\beta}\right) = 1; \quad \left(\frac{q}{\gamma}\right) = 1; \ldots.$$

Beweis. Ist die Congruenz

$$z^2 - q \equiv 0 \pmod{\alpha^m . \beta^n . \gamma^r \ldots}$$

gegeben, so sagt dieselbe aus, dass $z^2 - q$ ein Vielfaches von $(\alpha^m \beta^n \gamma^r \ldots)$, also jedenfalls ein Vielfaches von α, von β, von γ, ... einzeln. Die obige Congruenz setzt also jedenfalls die gleichzeitige Existenz der Congruenzen

$$z^2 - q \equiv 0 \pmod{\alpha}; \quad z^2 - q \equiv 0 \pmod{\beta};$$
$$z^2 - q \equiv 0 \pmod{\gamma} \ldots.$$

Diese Congruenzen können aber nach § 24 nur dann eine Lösung besitzen, wenn die Gleichungen

$$\left(\frac{q}{\alpha}\right) = 1; \quad \left(\frac{q}{\beta}\right) = 1; \quad \left(\frac{q}{\gamma}\right) = 1; \ldots.$$

gleichzeitig bestehen.

Man kann, wie man sieht, diese Umkehrung direct beweisen und dann den oben direct, aber auf complicirtem Wege bewiesenen Lehrsatz, indirect, aber sehr leicht beweisen.

Vorausgesetzt, nämlich, dass die Gleichungen

$$\left(\frac{q}{\alpha}\right) = 1; \quad \left(\frac{q}{\beta}\right) = 1; \quad \left(\frac{q}{\gamma}\right) = 1; \ldots.$$

stattfinden, so muss die Congruenz

$$z^2 - q \equiv 0 \pmod{\alpha^m \beta^n \gamma^r \ldots}$$

eine Lösung besitzen. Denn angenommen diese Congruenz habe keine Lösung, so hiesse dieses unter den Zahlen

$$0, 1, 2, \ldots, \alpha^m \beta^n \gamma^r \ldots . -1$$

findet sich keine einzige, welche, für z gesetzt, $z^2 - q$ zu einem Vielfachen von $\alpha^m \beta^n \gamma^r \ldots$ machen könnte. Es muss also für jeden Werth von z die Division von $z^2 - q$ durch $\alpha^m \beta^n \gamma^r \ldots$ immer irgend einen Rest R zurücklassen, welcher von Null verschieden ist.

Wählt man einen dieser Werthe von z, etwa z_1, zu welchem der Werth R_1, als Rest gehört, so besteht die Congruenz

$$z_1^2 - q \equiv R_1 \pmod{\alpha^m \beta^n \gamma^r \ldots},$$

also

$$z_1^2 - (q + R_1) \equiv 0 \pmod{\alpha^m \beta^n \gamma^r \ldots}.]$$

Hiermit schliessen wir die Theorie der Congruenzen zweiten Grades.

Kapitel V.

Ueber binomische Congruenzen.

---

§ 31. Ueber die Congruenz $x^m - 1 \equiv 0 \pmod{p}$, wenn p eine Primzahl ist.

Unter dem Namen „*binomische* Congruenz“ versteht man eine solche von der Gestalt

$$x^n - A \equiv 0 \pmod{p},$$

wobei n, A, p irgend welche ganze Zahlen sind. Wir beginnen mit dem einfachsten Falle, wenn $A = 1$, und p eine Primzahl ist.

Wir werden annehmen, es sei p von 2 verschieden, weil für $p = 2$, die Congruenz

$$x^n - A \equiv 0 \pmod{2}$$

nach § 20 auf eine Congruenz ersten Grades zurückgeführt wird.

In Bezug auf die Congruenz von der Gestalt

$$x^n - 1 \equiv 0 \pmod{p}$$

wollen wir zunächst folgenden Lehrsatz beweisen.

34. *Lehrsatz.* *Befriedigt eine Zahl die beiden Congruenzen*

$$x^m - 1 \equiv 0; \quad x^n - 1 \equiv 0 \pmod{p}$$

gleichzeitig, so befriedigt dieselbe Zahl auch die Congruenz

$$x^\omega - 1 \equiv 0 \pmod{p},$$

wenn ω *den grössten gemeinsamen Theiler von* m *und* n *bedeutet.*

Beweis. Es mag a eine Zahl sein, welche sowohl $x^m - 1 \equiv 0 \pmod{p}$, als auch $x^n - 1 \equiv 0 \pmod{p}$ befriedigt; wir erhalten dann

$$a^m \equiv 1; \quad a^n \equiv 1 \pmod{p}$$

und a muss relativ prim zu p sein, weil sonst

$$a^m \equiv 0 \pmod{p}$$

wäre.

Indem ω als grösster gemeinsamer Theiler von m und n vorausgesetzt war, erhalten wir in den Quotienten

$$\frac{m}{\omega}, \quad \frac{n}{\omega}$$

ganze Zahlen, die relativ prim zu einander sind. Sind aber $\frac{m}{\omega}$, $\frac{n}{\omega}$ relativ prim zu einander, so wird man eine Zahl z finden können, die der Congruenz ersten Grades

$$\frac{m}{\omega} z - 1 \equiv 0 \pmod{\frac{n}{\omega}}$$

genügt. Diese Congruenz sagt aus, dass die Differenz $\frac{m}{\omega} z - 1$ durch $\frac{n}{\omega}$ theilbar ist; bezeichnen wir den Quotienten dieser Division mit y, so finden wir

$$\frac{m}{\omega} z - 1 = \frac{n}{\omega} y,$$

woraus folgt

$$mz - ny = \omega \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (19)$$

Erhebt man die erste der beiden Congruenzen

$$a^m \equiv 1; \quad a^n \equiv 1 \pmod{p}$$

zur Potenz z, die zweite zur Potenz y, so erhält man

$$a^{mz} \equiv a^{ny} \pmod{p}.$$

Dividirt man beide Seiten dieser Congruenz durch a^{ny} (eine Zahl, welche zu p relativ prim ist, weil, wie wir gesehen haben, a relativ prim zu p sein muss), so verwandelt sich die Congruenz in:

$$a^{mz-ny} \equiv 1 \pmod{p},$$

oder, wenn man für $mz-ny$ seinen Werth ω aus (19) setzt, in:

$$a^{\omega} \equiv 1 \pmod{p}$$

was zu beweisen war.

Aus diesem Lehrsatze kann man ferner den folgenden herleiten.

35. *Lehrsatz.* a) *Die Lösungen einer Congruenz*

$$x^m - 1 \equiv 0 \pmod{p}$$

sind zugleich auch Lösungen von

$$x^{p-1} - 1 \equiv 0 \pmod{p}.$$

b) *Ist* ω *der grösste gemeinsame Theiler von* m *und* $p-1$, *so besitzt die Congruenz*

$$x^m - 1 \equiv 0 \pmod{p}$$

ω *Lösungen, welche aus der Congruenz*

$$x^{\omega} - 1 \equiv 0 \pmod{p}$$

sich ergeben.

Beweis. Der Congruenz $x^m - 1 \equiv 0 \pmod{p}$ können nur Zahlen genügen, die durch p nicht theilbar sind; weil für jedes x, welches ein Vielfaches von p ist, $x^m \equiv 0 \pmod{p}$ sein würde. Für jedes durch p nicht theilbares x besteht aber nach dem Fermat'schen Satze die Congruenz

$$x^{p-1} - 1 \equiv 0 \pmod{p}.$$

Folglich müssen alle Zahlen, welche die Congruenz $x^m - 1 \equiv 0 \pmod{p}$ befriedigen, zugleich auch der Congruenz $x^{p-1} - 1 \equiv 0 \pmod{p}$ genügen. Daraus ergiebt sich dann, nach dem vorhergehenden Lehrsatze, dass dieselben Zahlen auch die Congruenz

$$x^{\omega} - 1 \equiv 0 \pmod{p}$$

befriedigen, wenn ω den grössten gemeinsamen Theiler von m und $p-1$ bedeutet.

Ebenso leicht kann man sich, *umgekehrt*, überzeugen, dass alle Zahlen, welche die letzte Congruenz befriedigen, auch die Congruenz

$$x^m-1\equiv 0 \pmod{p}$$

befriedigen müssen.

Schreibt man die Congruenz $x^\omega-1\equiv 0 \pmod{p}$ in der Form $x^\omega\equiv 1 \pmod{p}$ und erhebt beide Seiten zur Potenz $\frac{m}{\omega}$ (es ist offenbar $\frac{m}{\omega}$ eine ganze Zahl, weil ω ein Theiler von m ist), so erhält man in der That $x^m\equiv 1 \pmod{p}$, oder $x^m-1\equiv 0 \pmod{p}$.

Somit werden beide Congruenzen

$$x^m-1\equiv 0;\quad x^\omega-1\equiv 0 \pmod{p}$$

durch ein und dieselben Zahlen befriedigt. Es bleibt uns daher nur noch zu zeigen übrig, dass diese Congruenzen wirklich ω Lösungen besitzen. Dieses lässt sich leicht an der Congruenz $x^\omega-1\equiv 0 \pmod{p}$ zeigen. Da ω ein Theiler von $p-1$ ist, so ist $\frac{p-1}{\omega}$ eine ganze Zahl; bezeichnen wir dieselbe mit n, so erhält man $p-1 = \omega n$. Man wird daher x^p-x in der Form

$$x^p-x = x(x^{n\omega}-1) = x\,[(x^\omega)^n-1^n]$$

darstellen können. In dieser Form erkennt man aber die Theilbarkeit von x^p-x durch $x^\omega-1$ sofort; weil die Differenz der Potenzen A^n-B^n bekanntlich immer durch die Differenz der Wurzeln $A-B$ theilbar ist.

Ist aber x^p-x durch $x^\omega-1$ ohne Rest theilbar, so hat die Congruenz $x^\omega-1\equiv 0 \pmod{p}$, nach Lehrsatz 26, ω Lösungen. Weil aber diese Congruenz nur durch Zahlen, welche der Congruenz $x^m-1\equiv 0 \pmod{p}$ genügen, befriedigt werden kann, so muss auch die letztere Congruenz ω Lösungen haben; was zu beweisen war.

Beispiel. Die Congruenz $x^{10}-1\equiv 0 \pmod{17}$, bei welcher 2 der grösste gemeinsame Theiler der Zahlen 10 und $17-1$ ist, hat nur zwei Lösungen, welche aus der Congruenz

$$x^2\equiv 1 \pmod{17}$$

gefunden werden.

Bemerkt man, dass dieser Congruenz die Zahlen 1 und $17-1 = 16$ genügen, so dass die Lösungen derselben

$$x \equiv 1 ; \quad x \equiv 16 \pmod{17}$$

sind, so kann man schliessen, dass auch die Lösungen der Congruenz

$$x^{10} - 1 \equiv 0 \pmod{17}$$

keine andere als

$$x \equiv 1 ; \quad x \equiv 16 \pmod{17}$$

sind.

Auf Grund des letzten Lehrsatzes wird somit die Lösung einer Congruenz $x^m - 1 \equiv 0 \pmod{p}$ auf die Lösung der Congruenz $x^\omega - 1 \equiv 0 \pmod{p}$ zurückgeführt, wobei ω ein Theiler von $p-1$ ist. Mit dieser letzteren Congruenz wollen wir uns nunmehr beschäftigen und beweisen zunächst folgenden

36. *Lehrsatz. Der Congruenz $x^\omega - 1 \equiv 0 \pmod{p}$, in welcher ω ein Theiler von $p-1$ ist, genügt eine Zahl*

$$\alpha = n^{\frac{p-1}{\omega}},$$

wenn n relativ prim zu p ist.

Beweis. Man hat nämlich, da $\alpha = n^{\frac{p-1}{\omega}}$ angenommen wird,

$$\alpha^\omega - 1 = n^{p-1} - 1.$$

Nach dem Fermat'schen Satze besteht aber, wenn n relativ prim zu p ist, die Congruenz

$$n^{p-1} - 1 \equiv 0 \pmod{p},$$

folglich auch

$$\alpha^\omega - 1 \equiv 0 \pmod{p};$$

was zu beweisen war.

Beispiel. Der Congruenz $x^5 - 1 \equiv 0 \pmod{11}$ genügen die Zahlen

$$2^{\frac{11-1}{5}} = 4; \quad 3^{\frac{11-1}{5}} = 9; \quad 4^{\frac{11-1}{5}} = 16; \ldots.$$

Auf diese Weise kann man mehrere Lösungen der Congruenz $x^\omega - 1 = 0 \pmod{p}$ finden. Was nun die Auffindung *aller* Lösungen dieser Congruenz betrifft, so beweisen wir diesbezüglich folgenden Lehrsatz.

37. *Lehrsatz. Befriedigt eine Zahl ϑ die Congruenz*

$$x^\omega - 1 \equiv 0 \pmod{p},$$

ohne eine der Congruenzen

$$x^\alpha - 1 \equiv 0; \; x^\beta - 1 \equiv 0; \ldots; \; x^\varrho - 1 \equiv 0 \pmod{p}$$

zu befriedigen, wenn

$$\alpha, \; \beta, \; \ldots, \; \varrho$$

Theiler von ω (die 1 mit inbegriffen) bedeuten, so werden alle ω-Lösungen der Congruenz durch die ω successiven Potenzen von ϑ, also

$$x \equiv \vartheta; \; x \equiv \vartheta^2; \; \ldots; \; x \equiv \vartheta^\omega \pmod{p}$$

erhalten.

Beweis. Man überzeugt sich leicht, dass wenn ϑ die Congruenz

$$x^\omega - 1 \equiv 0 \pmod{p}$$

befriedigt, derselben auch ϑ^n genügt, wenn n eine beliebige Zahl ist. Denn, wenn ϑ diese Congruenz befriedigt, so hat man $\vartheta^\omega - 1 \equiv 0 \pmod{p}$; also

$$\vartheta^\omega \equiv 1 \pmod{p}.$$

Erhebt man beide Seiten dieser Congruenz zur $n$ten Potenz, so erhält man $\vartheta^{n\omega} \equiv 1 \pmod{p}$, oder, was dasselbe ist:

$$\vartheta^{n\omega} - 1 \equiv 0 \pmod{p},$$

woraus erhellt, dass ϑ^n der Congruenz $x^\omega - 1 \equiv 0 \pmod{p}$ genügt.

Daraus folgt, dass $\vartheta, \vartheta^2, \ldots, \vartheta^\omega$ und somit auch alle durch die Congruenzen

$$x \equiv \vartheta; \quad x \equiv \vartheta^2; \quad \ldots; \quad x \equiv \vartheta^\omega \pmod{p} \quad . \quad . \quad (20)$$

definirten Zahlen die Congruenz

$$x^\omega - 1 \equiv 0 \pmod{p}$$

befriedigen.

Wir wollen nun beweisen, dass unter den Congruenzen (20) nicht zwei einander identisch sein können. Nehmen wir zu diesem Ende das Gegentheil an, dass nämlich irgend zwei, etwa

$$x \equiv \vartheta^m; \quad x \equiv \vartheta^n \pmod{p}$$

einander identisch seien, während m, n, als Exponenten von ϑ in den Congruenzen (20), grösser als 0 und nicht grösser als ω sein sollen. Es sei nun m grösser als n.

Indem wir zulassen, dass die beiden letztgenannten Congruenzen durch eine und dieselbe Zahl x befriedigt werden, erhalten wir

$$\vartheta^m \equiv \vartheta^n \pmod{p}$$

und durch Division beider Seiten durch ϑ^n (welches relativ prim zu p) — die Congruenz

$$\vartheta^{m-n} - 1 \equiv 0 \pmod{p}.$$

Diese Congruenz liefert, in Verbindung mit

$$\vartheta^\omega - 1 \equiv 0 \pmod{p},$$

welche nach Voraussetzung durch ϑ befriedigt wird, nach Lehrsatz 34 die neue Congruenz

$$\vartheta^{\omega'} - 1 \equiv 0 \pmod{p},$$

wobei ω' den grössten gemeinsamen Theiler von $m-n$ und ω bedeutet. Da ω' ein Theiler von $m-n$ ist, so kann nicht $\omega' = \omega$ sein, weil m und n grösser als 0 und nicht grösser als ω sind und somit $m-n < \omega$. Ist aber $\omega' < \omega$ und ein Theiler von ω, so muss ω' eine der Zahlen

$$\alpha, \beta, \ldots, \varrho$$

sein, welche alle Theiler von ω darstellen. Die Congruenz

$$\vartheta^{\omega'} - 1 \equiv 0$$

muss also eine jener Congruenzen

$$\vartheta^{\alpha}-1 \equiv 0; \quad \vartheta^{\beta}-1 \equiv 0; \quad \ldots; \quad \vartheta^{\gamma}-1 \equiv 0 \pmod{p}$$

sein, welche nach der Voraussetzung nicht stattfinden können.

Es können folglich nicht zwei der ω Congruenzen

$$x \equiv \vartheta; \quad x \equiv \vartheta^2; \quad \ldots; \quad x \equiv \vartheta^{\omega} \pmod{p}$$

einander identisch sein; dieselben liefern daher alle ω Lösungen der Congruenz

$$x^{\omega}-1 \equiv 0 \pmod{p},$$

was wir beweisen wollten.

Beispiel. Um alle Lösungen der Congruenz

$$x^6-1 \equiv 0 \pmod{13}$$

zu finden, müssen wir eine solche Zahl aufsuchen, welche diese Congruenz befriedigt, ohne die Congruenzen

$$x-1 \equiv 0; \quad x^2-1 \equiv 0; \quad x^3-1 \equiv 0 \pmod{13}$$

zu befriedigen. Indem wir nun finden, dass die Zahl 4 eine solche Eigenschaft besitzt, erhalten wir alle Lösungen der Congruenz $x^6-1 \equiv 0 \pmod{13}$ durch die Congruenzen

$$x \equiv 4; \; x \equiv 4^2; \; x \equiv 4^3; \; x \equiv 4^4; \; x \equiv 4^5; \; x \equiv 4^6 \pmod{13},$$

oder:

$$x \equiv 4; \; x \equiv 3; \; x \equiv 12; \; x \equiv 9; \; x \equiv 10; \; x \equiv 1 \pmod{13}.$$

---

§ 32. Ueber die Congruenz $x^m-A \equiv 0 \pmod{p}$, wenn p eine Primzahl ist.

Wir gehen jetzt zu den allgemeinern Congruenzen von der Gestalt

$$x^m-A \equiv 0 \pmod{p}$$

über, wobei A eine beliebige, durch p nicht theilbare Zahl bedeutet, während p eine Primzahl, die wir wiederum, von 2 verschieden voraussetzen, sein soll.

Ueber Congruenzen von dieser Gestalt beweisen wir folgenden Lehrsatz.

38. *Lehrsatz.* a) *Die Congruenz* $x^m - A \equiv 0 \pmod{p}$ *ist nur dann möglich, wenn*

$$A^{\frac{p-1}{\omega}} \equiv 1 \pmod{p},$$

während ω *der grösste gemeinsame Theiler von* $p-1$ *und* m *ist.*

b) *Ist die Congruenz* $x^m - A \equiv 0 \pmod{p}$ *überhaupt möglich, so besitzt dieselbe* ω *Lösungen, welche aus der Congruenz*

$$x^\omega - A^\pi \equiv 0 \pmod{p}$$

sich ergeben, wenn π *eine Zahl ist, welche der Bedingung*

$$\frac{m}{\omega}\pi \equiv 1 \left(\text{mod.}\ \frac{p-1}{\omega}\right)$$

genügt.

Beweis. Es war A durch p untheilbar vorausgesetzt; daher kann eine die Congruenz $x^m - A \equiv 0 \pmod{p}$, oder $x^m \equiv A \pmod{p}$ befriedigende Zahl x nicht ein Vielfaches von p sein; weil sonst $x^m \equiv 0 \pmod{p}$ wäre und wir aus $x^m \equiv A \pmod{p}$ für A die Congruenz $A \equiv 0 \pmod{p}$ erhalten hätten. Ist aber x durch p nicht theilbar, so erhalten wir nach dem *Fermat*'schen Satze

$$x^{p-1} \equiv 1 \pmod{p}.$$

Erhebt man beide Seiten dieser Congruenz zur Potenz $\frac{m}{\omega}$ und beide Seiten der Congruenz $x^m \equiv A \pmod{p}$ zur Potenz $\frac{p-1}{\omega}$ (die Exponenten $\frac{m}{\omega}$, $\frac{p-1}{\omega}$ sind ganze Zahlen, weil ω gemeinsamer Theiler von m und $p-1$ ist), so erhält man

$$x^{\frac{m(p-1)}{\omega}} \equiv 1; \quad x^{\frac{m(p-1)}{\omega}} \equiv A^{\frac{p-1}{\omega}} \pmod{p};$$

woraus folgt

$$A^{\frac{p-1}{\omega}} \equiv 1 \pmod{p}.$$

Damit also die Congruenz $x^m - A \equiv 0 \pmod{p}$ möglich sein soll, ist nothwendig, dass A der Congruenz

$$A^{\frac{p-1}{\omega}} \equiv 1 \pmod{p} \quad . \quad . \quad . \quad . \quad . \quad (21)$$

Genüge leistet.

Nehmen wir nun an, diese Bedingung sei erfüllt, so können wir beweisen, dass dann alle Zahlen, welche die Congruenz

$$x^m \equiv A \pmod{p}$$

befriedigen, zugleich auch der Congruenz

$$x^\omega \equiv A^\pi \pmod{p}$$

genügen, wenn π eine durch die Congruenz

$$\frac{m}{\omega}\pi \equiv 1 \left(\text{mod.}\ \frac{p-1}{\omega}\right)$$

definirte Zahl bedeutet.

Da nämlich ω den grössten gemeinsamen Theiler von m und $p-1$ bedeutet, so erhalten wir in

$$\frac{m}{\omega},\ \frac{p-1}{\omega}$$

ganze Zahlen, welche relativ prim zu einander sind. Man kann aber immer, wenn $\frac{m}{\omega}$, $\frac{p-1}{\omega}$ relativ prim zu einander sind, eine Zahl π finden, welche die Congruenz

$$\frac{m}{\omega}\pi \equiv 1 \left(\text{mod.}\ \frac{p-1}{\omega}\right)$$

befriedigt. Für diese Zahl π wird, mit anderen Worten, die Differenz

$$\frac{m}{\omega}\pi - 1$$

durch $\frac{p-1}{\omega}$ theilbar sein. Bezeichnen wir den Quotienten dieser Division mit ϱ, so erhalten wir

$$\frac{m}{\omega}\pi - 1 = \varrho\frac{p-1}{\omega}$$

oder, so geschrieben:

$$m\pi - \varrho(p-1) = \omega \quad . \quad . \quad . \quad . \quad . \quad (22)$$

Auf Grund dieser Gleichung kann man sofort zeigen, dass zugleich mit

$$x^m \equiv A \pmod{p}$$

auch

$$x^\omega \equiv A^\pi \pmod{p}$$

bestehen muss.

Erheben wir nämlich beide Seiten der Congruenz

$$x^m \equiv A \pmod{p}$$

zur π^{ten} Potenz, so erhalten wir

$$x^{m\pi} \equiv A^\pi \pmod{p};$$

erhebt man zugleich beide Seiten der aus dem *Fermat*'schen Satze sich ergebenden Congruenz

$$x^{p-1} \equiv 1 \pmod{p}$$

zur ϱ^{ten} Potenz, so erhält man:

$$x^{\varrho(p-1)} \equiv 1, \quad \text{oder} \quad 1 \equiv x^{\varrho(p-1)} \pmod{p}.$$

Multiplicirt man beide Congruenzen

$$x^{m\pi} \equiv A^\pi; \quad 1 \equiv x^{\varrho(p-1)} \pmod{p}$$

gliedweise mit einander, so erhält man

$$x^{m\pi} \equiv A^\pi x^{\varrho(p-1)} \pmod{p},$$

woraus nach Division beider Seiten durch $x^{\varrho(p-1)}$, welche Zahl nach Voraussetzung relativ prim zu p ist, sich

$$x^{m\pi-\varrho(p-1)} \equiv A^\pi \pmod{p}$$

ergiebt. Ersetzt man darin die Zahl $m\pi-\varrho(p-1)$ durch die (nach 22) ihr gleiche Zahl ω, so erhält man endlich

$$x^\omega \equiv A^\pi \pmod{p},$$

was zu beweisen war.

Haben wir uns somit überzeugt, dass die Congruenz

$x^m \equiv A \pmod{p}$ keine anderen Lösungen als diejenigen der Congruenz $x^\omega \equiv A^\pi \pmod{p}$ besitzen kann, so können wir auch den zweiten Theil unseres Lehrsatzes beweisen. Wir beweisen nämlich, dass die Congruenz

$$x^\omega \equiv A^\pi \pmod{p}$$

wirklich ω Lösungen besitzt und dass alle diese Lösungen zugleich auch die Congruenz

$$x^m \equiv A \pmod{p}$$

befriedigen.

Wir verfahren, um uns von der Richtigkeit dieser Behauptung zu überzeugen, wiederum nach der im § 21 angegebenen Methode, indem wir den Rest suchen, welcher bei der Division von $x^p - x$ durch $x^\omega - A^\pi$ verbleibt. Man findet diesen Rest sehr leicht, wenn man bemerkt, dass man $x^p - x$ so schreiben kann:

$$\left[(x^\omega)^{\frac{p-1}{\omega}} - (A^\pi)^{\frac{p-1}{\omega}}\right] x + \left[A^{\frac{\pi(p-1)}{\omega}} - 1\right] x.$$

In dieser Form erkennt man sofort, dass der erste Theil

$$\left[(x^\omega)^{\frac{p-1}{\omega}} - (A^\pi)^{\frac{p-1}{\omega}}\right] x$$

durch $x^\omega - A^\pi$ theilbar ist, woraus sich somit

$$\left(A^{\frac{\pi(p-1)}{\omega}} - 1\right) x$$

als der gesuchte Rest ergiebt.

Der Coefficient $A^{\frac{\pi(p-1)}{\omega}} - 1$ ist aber hier durch p theilbar, weil die Erhebung beider Seiten von (21) zur π^{ten} Potenz die Congruenz

$$A^{\frac{\pi(p-1)}{\omega}} \equiv 1 \pmod{p}$$

liefert. Nach Lehrsatz 26 besitzt daher die Congruenz

$$x^\omega \equiv A^\pi \pmod{p}$$

wirklich ω Lösungen.

Es bleibt uns nur noch zu beweisen übrig, dass alle Lösungen der Congruenz

$$x^{\omega} \equiv A^{\pi} \pmod{p}$$

auch die Congruenz

$$x^{m} \equiv A \pmod{p}$$

befriedigen.

Erheben wir beide Seiten der vorletzten Congruenz zur Potenz $\frac{m}{\omega}$, so erhalten wir

$$x^{m} \equiv A^{\frac{\pi m}{\omega}} \pmod{p}.$$

Subtrahirt man A von beiden Seiten dieser Congruenz, so erhält man

$$x^{m} - A \equiv A^{\frac{\pi m}{\omega}} - A \pmod{p},$$

oder, so geschrieben:

$$x^{m} - A \equiv A\left(A^{\frac{\pi m - \omega}{\omega}} - 1\right) \pmod{p}.$$

Setzt man hierin für $\pi m - \omega$ den aus (22) sich ergebenden Werth $\varrho(p-1)$, so erhält man

$$x^{m} - A \equiv A\left(A^{\frac{\varrho(p-1)}{\omega}} - 1\right) \pmod{p} \quad . \; . \; . \; . \; (23)$$

Nach (21) befriedigt nun A die Congruenz

$$A^{\frac{p-1}{\omega}} \equiv 1 \pmod{p},$$

welche durch Erhebung beider Seiten zur Potenz ϱ in

$$A^{\frac{\varrho(p-1)}{\omega}} \equiv 1 \pmod{p},$$

oder

$$A^{\frac{\varrho(p-1)}{\omega}} - 1 \equiv 0 \pmod{p}$$

übergeht. Infolge dieser letzteren, geht aber die Congruenz (23) in

$$x^{m} - A \equiv 0 \pmod{p}$$

über; was noch zu beweisen übrig geblieben war.

Beispiel. In der Congruenz

$$x^8 - 3 \equiv 0 \pmod{11}$$

ist 2 der grösste gemeinsame Theiler von 8 und 11−1. Damit also die Congruenz wirklich Lösungen habe, ist nothwendig, dass

$$3^{\frac{11-1}{2}} \equiv 1 \pmod{11}$$

erfüllbar sei. Diese Bedingung ist aber wirklich erfüllt, weil

$$3^{\frac{11-1}{2}} = 3^5 = 243 \text{ und } 243 \equiv 1 \pmod{11}.$$

ist.

Man findet auch die Lösungen unserer Congruenz in der That aus der Congruenz

$$x^2 - 3^\pi \equiv 0 \pmod{11},$$

wobei π durch die Bedingung

$$\frac{8}{2}\pi \equiv 1 \left(\text{mod. } \frac{11-1}{2}\right),$$

also

$$4\pi \equiv 1 \pmod{5}$$

definirt ist.

Indem wir diese Congruenz nach der in § 15 gezeigten Methode lösen, finden wir

$$\pi \equiv 4^{5-2} \equiv 64 \pmod{5}.$$

Daraus ersieht man, dass $\pi = 4$ gesetzt werden kann. Infolgedessen geht die Congruenz

$$x^2 - 3^\pi \equiv 0 \pmod{11}$$

in

$$x^2 - 81 \equiv 0 \pmod{11}$$

über, der offenbar die Zahlen $x = 9$ und $x = 11 - 9 = 2$ genügen. Die Lösungen der Congruenz

$$x^8 - 3 \equiv 0 \pmod{11}$$

sind somit

$$x \equiv 2; \quad x \equiv 9 \pmod{11}.$$

Aus den über die Congruenzen von der Gestalt

$$x^m - A \equiv 0 \pmod{p}$$

bewiesenen Lehrsätzen wollen wir folgenden Lehrsatz herleiten.

39. *Lehrsatz. Die Congruenz*

$$x^m + 1 \equiv 0 \pmod{p}$$

hat keine Lösung, wenn $p-1$ *nach Befreiung von gemeinsamen Theilern mit* m *auf eine ungerade Zahl führt.*

Im entgegengesetzten Falle, besitzt die Congruenz ω *Lösungen, wenn* ω *den grössten gemeinsamen Theiler von* $p-1$ *und* ω *bedeutet; und diese Lösungen werden aus der Congruenz*

$$x^\omega + 1 \equiv 0 \pmod{p}$$

gefunden.

Beweis. Nach Lehrsatz 38 wissen wir, dass, damit die Congruenz $x^m + 1 \equiv 0 \pmod{p}$ möglich werde, es nothwendig ist, dass die Congruenz

$$(-1)^{\frac{p-1}{\omega}} \equiv 1 \pmod{p}$$

bestehe. Dieses ist aber unmöglich, wenn $\frac{p-1}{\omega}$ eine ungerade Zahl ist; es muss folglich der Quotient der Division von $p-1$ durch den grössten gemeinsamen Theiler ω von $p-1$ und m eine gerade Zahl sein.

Ist aber $\frac{p-1}{\omega}$ eine gerade Zahl, so wird die Bedingung

$$(-1)^{\frac{p-1}{\omega}} \equiv 1 \pmod{p}$$

erfüllt und die Congruenz

$$x^m + 1 \equiv 0 \pmod{p}$$

hat in diesem Falle, nach unserem bereits bewiesenen Lehrsatze, ω Lösungen und diese Lösungen werden durch die Congruenz

$$x^\omega - (-1)^\pi \equiv 0 \pmod{p}$$

ermittelt, wobei π durch die Congruenz

$$\frac{m}{w}\pi \equiv 1 \left(\text{mod. } \frac{p-1}{\omega}\right)$$

definirt ist.

Da nun in dieser letzten Congruenz der Modul eine gerade Zahl ist, während die rechte Seite durch 2 untheilbar ist, so muss auch die linke Seite relativ prim zu 2 sein. Daraus folgt, dass π eine ungerade Zahl sein muss, infolge dessen die Congruenz

$$x^\omega - (-1)^\pi \equiv 0 \text{ (mod. } p),$$

durch welche die Lösungen der Congruenz

$$x^m + 1 \equiv 0 \text{ (mod. } p)$$

bestimmt werden, in

$$x^\omega + 1 \equiv 0 \text{ (mod. } p)$$

sich verwandelt.

So haben wir uns von der Richtigkeit des ausgesprochenen Lehrsatzes überzeugt.

Beispiele. 1) Aus unserem Lehrsatze schliessen wir, dass die Congruenz

$$x^4 + 1 \equiv 0 \text{ (mod. 13)}$$

keine Lösung hat; weil der grösste gemeinsame Theiler von 4 und 13—1 die Zahl 4 ist und der Quotient der Division von 13—1 durch 4 die *ungerade* Zahl 3 liefert.

2) Dagegen hat die Congruenz

$$x^9 + 1 \equiv 0 \text{ (mod. 13)}$$

drei Lösungen, weil als grösster gemeinsamer Theiler von 9 und 13—1 sich 3 ergiebt und die Division von 13—1 durch 3 die gerade Zahl 4 zum Quotienten liefert.

Die drei Lösungen erhält man aus der Congruenz

$$x^3 + 1 \equiv 0 \text{ (mod. 13)}.$$

---

§ 33. **Ueber die Congruenz $x^m - A \equiv 0$ (mod. N), wenn N eine zusammengesetzte Zahl ist.**

Bisher haben wir uns bei der Behandlung der Congruenz

$$x^m - A \equiv 0 \pmod{p}$$

auf den Fall beschränkt, wenn der Modul p eine Primzahl ist. Wir wenden uns nunmehr zu dem allgemeinen Fall

$$x^m - A \equiv 0 \pmod{N},$$

wenn der Modul N eine zusammengesetzte Zahl ist.

Wir nehmen an, dass der Modul N relativ prim zu m und zu A ist und beweisen für diesen Fall, dass wenn die Congruenz

$$x^m - A \equiv 0 \pmod{p},$$

deren Modul p eine der in N enthaltenen Primzahlen bedeutet, befriedigt werden kann, dann auch der Congruenz

$$x^m - A \equiv 0 \pmod{N}$$

Genüge geleistet werden kann.

Wir beginnen mit dem speciellen Falle

$$x^m - A \equiv 0 \pmod{M},$$

wenn der Modul M eine Potenz einer Primzahl, etwa

$$M = \alpha^\mu,$$

wobei α eine Primzahl, welche nicht Theiler von m oder von A ist, bedeutet. Wir wollen zeigen, wie man aus einer Lösung der Congruenz

$$x^m - A \equiv 0 \pmod{\alpha}$$

Lösungen der Congruenzen

$$x^m - A \equiv 0 \pmod{\alpha^2}; \quad x^m - A \equiv 0 \pmod{\alpha^3}; \; \ldots \,.$$

herleiten kann.

Es mag a eine Zahl sein, welche die Congruenz

$$x^m - A \equiv 0 \pmod{\alpha}$$

befriedigt; es kann a nicht durch α theilbar sein, weil A

nach Voraussetzung durch α untheilbar war. Um eine Zahl zu finden, welche die Congruenz

$$x^m - A \equiv 0 \pmod{\alpha^2}$$

befriedigt, setzen wir $x = a + \alpha z$ und suchen die Zahl z so zu bestimmen, dass die Bedingung

$$(a + \alpha z)^m - A \equiv 0 \pmod{\alpha^2}$$

erfüllt werde.

Die letzte Congruenz kann man so schreiben:

$$a^m - A + m a^{m-1} \alpha z + \frac{m(m-1)}{1 \,.\, 2} a^{m-2} \alpha^2 z^2 + \ldots + \alpha^m z^m \equiv 0 \pmod{\alpha^2}$$

und man sieht sofort, dass hierin α ein gemeinsamer Theiler aller Glieder der Congruenz und ihres Moduls ist. Denn da a die Congruenz $x^m - A \equiv 0 \pmod{\alpha}$ befriedigt, so muss die Differenz $a^m - A$ ein Vielfaches von α sein; alle übrigen Glieder unserer Congruenz und der Modul enthalten aber α explicite als Factor. Dividiren wir daher alle Glieder und den Modul durch α, so erhalten wir

$$\frac{a^m - A}{\alpha} + m a^{m-1} z + \frac{m(m-1)}{1 \,.\, 2} a^{m-2} \alpha z^2 + \ldots + \alpha^{m-1} z^m \equiv 0 \pmod{\alpha}.$$

Subtrahiren wir von dieser die offenbar identische Congruenz

$$\frac{m(m-1)}{1 \,.\, 2} a^{m-2} \alpha z^2 + \ldots + \alpha^{m-1} z^m \equiv 0 \pmod{\alpha},$$

so erhalten wir die Congruenz

$$\frac{a^m - A}{\alpha} + m a^{m-1} z \equiv 0 \pmod{\alpha},$$

welche, als Congruenz ersten Grades in Bezug auf z, leicht gelöst werden kann.

Man überzeugt sich leicht, dass diese Congruenz immer eine Lösung besitzt; weil der Coefficient von z, als Product von m und einer Potenz von a, welche beide relativ prim zu α vorausgesetzt waren, selbst relativ prim zum Modul α ist. Wir wissen aber, dass eine Congruenz ersten Grades in diesem Falle immer eine Lösung besitzt.

Die Lösung der Congruenz

$$\frac{a^m - A}{\alpha} + m a^{m-1} z \equiv 0 \pmod{\alpha}$$

liefert somit eine Zahl z, mit Hülfe deren man diejenige Zahl $x = b$, welche die Congruenz

$$x^m - A \equiv 0 \pmod{\alpha^2}$$

befriedigt, in der Gestalt

$$b = a + \alpha z$$

darstellen kann.

Man kann aber leicht zeigen, dass man vermittelst einer solchen Zahl b, welche die Congruenz

$$x^m - A \equiv 0 \pmod{\alpha^2}$$

befriedigt, immer eine Zahl $x = c$ finden kann, durch welche die Congruenz

$$x^m - A \equiv 0 \pmod{\alpha^3}$$

befriedigt ist.

Wir setzen zu diesem Zwecke in der letzten Congruenz

$$x = b + \alpha^2 u$$

und erhalten für u die Bestimmung

$$(b + \alpha^2 u)^m - A \equiv 0 \pmod{\alpha^3}.$$

Indem wir wiederum

$$(b + \alpha^2 u)^m$$

nach dem binomischen Satze entwickeln, alle Glieder der Congruenz und den Modul durch α^2 dividiren und die Glieder, welche noch dann Vielfache von α bleiben, fortlassen, erhalten wir, ganz analog wie oben, für die Bestimmung von u die Congruenz ersten Grades

$$\frac{b^m - A}{\alpha^2} + m b^{m-1} u \equiv 0 \pmod{\alpha}.$$

Bestimmen wir daraus u, was offenbar wieder immer möglich ist, weil auch hier der Coefficient von u relativ prim zum Modul ist, so finden wir eine Zahl $x = c$, welche der Congruenz

$$x^m - A \equiv 0 \pmod{\alpha^3}$$

genügt, vermittelst Gleichung

$$x = b + \alpha^2 u.$$

Fahren wir auf diese Weise fort, so erhalten wir ebenso die Lösungen der Congruenzen

$$x^m - A \equiv 0 \pmod{\alpha^4}; \quad x^m - A \equiv 0 \pmod{\alpha^5} \text{ u. s. f.}$$

Beispiel. Wir wollen die Lösung der Congruenz

$$x^5 - 2 \equiv 0 \pmod{3^2}$$

auffinden.

Wir suchen zuerst die Lösung von

$$x^5 - 2 \equiv 0 \pmod{3},$$

welche, nach Lehrsatz 38, auf

$$x - 2^\pi \equiv 0 \pmod{3}$$

zurückgeführt wird, wobei π durch die Bedingung

$$5\pi \equiv 1 \pmod{2}$$

bestimmt wird.

Bemerkt man, dass diese Bedingung durch $\pi = 1$ erfüllt wird, so erhält man

$$x - 2 \equiv 0 \pmod{3}$$

als Lösung der Congruenz

$$x^5 - 2 \equiv 0 \pmod{3}.$$

Nachdem wir gefunden haben, dass diese Congruenz durch $x = 2$ befriedigt wird, setzen wir, um die Lösung von

$$x^5 - 2 \equiv 0 \pmod{3^2}$$

zu finden,

$$x = 2 + 3z,$$

wobei z aus der Bedingung

$$\frac{2^5 - 2}{3} + 5 \,.\, 2^{5-1} \,.\, z \equiv 0 \pmod{3},$$

oder

$$10 + 80z \equiv 0 \pmod{3}$$

bestimmt wird.

Nach Division beider Seiten durch 10, welche Zahl relativ prim zum Modul 3 ist, erhalten wir

$$8z \equiv -1 \pmod{3}.$$

Unter den Zahlen, welche diese Congruenz befriedigen findet sich $z = 1$; dieser Werth, für z genommen, liefert die Zahl

$$x = 2 + 3z = 5,$$

welche die Congruenz

$$x^5 - 2 \equiv 0 \pmod{3^2}$$

befriedigt.

Wir gehen jetzt zu dem allgemeinen Falle

$$x^m - A \equiv 0 \pmod{N}$$

über, wobei N eine beliebige zusammengesetzte Zahl bedeutet, welche jedoch zu m und zu A relativ prim vorausgesetzt wird.

Wir wollen beweisen, dass wenn N aus dem Producte von Potenzen der Primzahlen

$$\alpha, \beta, \gamma, \ldots.$$

besteht, für welche die Congruenzen

$$x^m - A \equiv 0 \pmod{\alpha}; \quad x^m - A \equiv 0 \pmod{\beta};$$
$$x^m - A \equiv 0 \pmod{\gamma}; \ldots.$$

Lösungen besitzen, man immer eine Lösung der Congruenz

$$z^m - A \equiv 0 \pmod{N}$$

finden kann.

Ist

$$N = \alpha^\lambda \ \beta^\mu \ \gamma^\nu \ \ldots.,$$

so finden wir zunächst, nach der auseinandergesetzten Methode, Zahlen, welche die Congruenzen

$$x^m - A \equiv 0 \pmod{\alpha^\lambda}; \quad x^m - A \equiv 0 \pmod{\beta^\mu};$$
$$x^m - A \equiv 0 \pmod{\gamma^\nu} \ldots.$$

befriedigen.

Es mögen diese Zahlen mit

$$\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \ldots.$$

bezeichnet werden.

Nach Lehrsatz 13 werden dann auch alle Zahlen, welche durch die Congruenz

$$x \equiv \mathfrak{A} \pmod{\alpha^\lambda}$$

definirt sind, ebenfalls die Congruenz

$$x^m - A \equiv 0 \pmod{\alpha^\lambda}$$

befriedigen; ebenso werden alle durch

$$x \equiv \mathfrak{B} \pmod{\beta^\mu}$$

definirten Zahlen die Congruenz

$$x^m - A \equiv 0 \pmod{\beta^\mu}$$

befriedigen; u. s. f.

In § 30 haben wir aber gezeigt, wie man eine Zahl finden kann, welche zugleich alle Congruenzen

$$x \equiv \mathfrak{A} \pmod{\alpha^\lambda}; \quad x \equiv \mathfrak{B} \pmod{\beta^\mu}; \quad x \equiv \mathfrak{C} \pmod{\gamma^\nu}; \; \ldots .$$

also auch alle Congruenzen

$$x^m - A \equiv 0 \pmod{\alpha^\lambda}; \quad x^m - A \equiv 0 \pmod{\beta^\mu}; \quad x^m - A \equiv 0 \pmod{\gamma^\nu}; \; \ldots .$$

befriedigt.

Da nun $\alpha, \beta, \gamma, \ldots.$ von einander verschiedene Primzahlen bedeuten, so sind die Moduli $\alpha^\lambda, \beta^\mu, \gamma^\nu, \ldots.$ relativ prim zu einander und in diesem Falle folgt aus diesen Congruenzen, nach § 9, die Congruenz

$$x^m - A \equiv 0 \pmod{\alpha^\lambda \beta^\mu \gamma^\nu \ldots.}.$$

Somit haben wir also eine die Congruenz

$$x^m - A \equiv 0 \pmod{\alpha^\lambda \beta^\mu \gamma^\nu \ldots.}$$

befriedigende Zahl dadurch gefunden, dass wir vorerst eine Zahl aufgesucht haben, welche den Congruenzen

$$x \equiv \mathfrak{A} \pmod{\alpha^\lambda}; \quad x \equiv \mathfrak{B} \pmod{\beta^\mu}; \quad x \equiv \mathfrak{C} \pmod{\gamma^\nu}; \; \ldots .$$

gleichzeitig genügt, wobei

$$\mathfrak{A}, \; \mathfrak{B}, \; \mathfrak{C}, \; \ldots .$$

durch die Bedingungen

$$\begin{aligned} \mathfrak{A}^m - A &\equiv 0 \pmod{\alpha^\lambda}, \\ \mathfrak{B}^m - A &\equiv 0 \pmod{\beta^\mu}, \\ \mathfrak{C}^m - A &\equiv 0 \pmod{\gamma^\nu}, \\ &\vdots \end{aligned}$$

bestimmt sind.

Kapitel VI.

Ueber Congruenzen von der Gestalt

$a^x \equiv A \pmod{p}$.

§ 34. Ueber die Congruenz $a^x \equiv A \pmod{p}$ im Allgemeinen und insbesondere über die Congruenz $a^x \equiv 1 \pmod{p}$.

Wir haben uns bis jetzt immer mit solchen Congruenzen, welche aus einer ganzen rationalen Function bestehen, beschäftigt, und aus diesen haben wir die bemerkenswerthesten, nämlich: die Congruenzen der ersten zwei Grade und die binomischen Congruenzen, eingehender untersucht. Jetzt gehen wir zu Congruenzen über, welche die Unbekannte als Exponenten enthalten. Unter diesen Congruenzen ist die bemerkenswertheste

$$a^x \equiv A \pmod{p},$$

wobei p eine, weder in a, noch in A als Theiler enthaltene, sonst aber beliebige Primzahl bedeutet. Mit der Untersuchung dieser Congruenz wollen wir uns jetzt beschäftigen. Es ist leicht in Bezug auf dieselbe folgenden Lehrsatz zu beweisen.

40. *Lehrsatz. Befriedigt eine Zahl α die Congruenz*

$$a^x \equiv A \pmod{p},$$

so befriedigt dieselbe Congruenz auch jede Zahl, welche congruent α nach dem Modul $p-1$ ist.

Beweis. Ist eine Zahl z congruent α nach dem Mo-

dul $p-1$, so ist $z-\alpha$ durch $p-1$ theilbar. Bezeichnen wir den Quotienten der Division von $z-\alpha$ durch $p-1$ mit ϱ, so erhalten wir

$$z-\alpha = (p-1)\varrho,$$

woraus folgt

$$a^{z-\alpha} = a^{(p-1)\varrho}.$$

Nach dem *Fermat*'schen Satze ist aber a^{p-1} und somit auch $a^{(p-1)\varrho} = (a^{p-1})^{\varrho}$ congruent 1 nach Modul p, folglich ist

$$a^{z-\alpha} \equiv 1 \pmod{p}.$$

Haben wir nun, nach der Voraussetzung

$$a^{\alpha} \equiv A \pmod{p},$$

so erhalten wir durch gliedweise Multiplication dieser letzten Congruenz mit der vorhergehenden:

$$a^{z} \equiv A \pmod{p},$$

was zu beweisen war.

Aus dem eben bewiesenen Lehrsatze folgt, dass wenn *eine* Zahl die Congruenz

$$a^{x} \equiv A \pmod{p}$$

befriedigt, dieselbe Congruenz auch unendlich viele andere Zahlen befriedigen, welche der ersten nach dem Modul $p-1$ congruent sind.

Alle solche Zahlen, welche einander nach Modul $p-1$ congruent sind, fassen wir als eine Lösung der Congruenz

$$a^{x} \equiv A \pmod{p}$$

auf.

In dieser Bedeutung hat dann die Congruenz

$$a^{x} \equiv A \pmod{p}$$

so viele Lösungen, als es ganze positive Zahlen giebt, welche kleiner als $p-1$, welche also untereinander nach Modul $p-1$ nicht congruent (incongruent) *sind, und die Congruenz befriedigen* *).

---

*) Man gelangt zu dieser Auffassung, wenn man ganz analoge

Diese Lösungen werden durch

$$x \equiv \alpha_1; \quad x \equiv \alpha_2; \quad \ldots\ldots; \quad x \equiv \alpha_n \pmod{p-1}$$

dargestellt, wobei

$$\alpha_1, \ \alpha_2, \ \ldots\ldots, \ \alpha_n$$

positive Zahlen, welche kleiner als $p-1$ sind und die Congruenz

$$a^x \equiv A \pmod{p}$$

befriedigen, bedeuten.

Nachdem wir gezeigt haben, wie die Lösungen der Congruenz

$$a^x \equiv A \pmod{p}$$

zu zählen sind, wollen wir zur wirklichen Bestimmung ihrer Anzahl schreiten und beginnen dabei mit dem speciellen Falle $A = 1$.

Bezüglich der Congruenz

$$a^x \equiv 1 \pmod{p}$$

kann man folgende Lehrsätze leicht beweisen.

41. *Lehrsatz. Befriedigt $x = \alpha$ die Congruenz*

$$a^x \equiv 1 \pmod{p},$$

so befriedigt auch jedes Vielfache von α dieselbe Congruenz.

Beweis. Wenn der Werth $x = \alpha$ die Congruenz

$$a^x \equiv 1 \pmod{p}$$

befriedigt, so besteht:

$$a^\alpha \equiv 1 \pmod{p}.$$

Erhebt man beide Seiten dieser Congruenz zu irgend welcher, etwa n^{ter} Potenz, so erhält man wieder

$$a^{n\alpha} \equiv 1 \pmod{p},$$

woraus ersichtlich ist, dass auch $x = n\alpha$ die Congruenz

$$a^x \equiv 1 \pmod{p}$$

befriedigt.

Ueberlegungen, wie wir sie in § 12, um die Anzahl der Lösungen der Congruenz $f(x) \equiv 0 \pmod{p}$ zu definiren, gebraucht haben, auch in Bezug auf die Lösungen der Congruenz $a^x \equiv A \pmod{p}$ anstellt.

42. Lehrsatz. *Befriedigt eine Zahl α die Congruenz*

$$a^x \equiv 1 \pmod{p},$$

so befriedigt auch der grösste gemeinsame Theiler von α und $p-1$ dieselbe Congruenz.

Beweis. Man kann diesen Lehrsatz leicht aus dem 35ten, über die binomische Congruenz

$$x^m - 1 \equiv 0 \pmod{p}$$

bewiesenen Lehrsatze herleiten, nach welchem jede diese Congruenz befriedigende Zahl a zugleich auch die Congruenz

$$x^\omega - 1 \equiv 0 \pmod{p}$$

befriedigen muss, wenn ω den grössten gemeinsamen Theiler von m und $p-1$ bedeutet. Daraus folgt nämlich unmittelbar, dass zugleich mit

$$a^m \equiv 1 \pmod{p} \text{ auch } a^\omega \equiv 1 \pmod{p}$$

besteht; wodurch unser Lehrsatz bewiesen ist.

43. Lehrsatz. *Die kleinste unter den Zahlen, welche die Congruenz*

$$a^x \equiv 1 \pmod{p}$$

befriedigen, die Null ausgenommen, ist ein Theiler von $p-1$; alle übrigen dieser Zahlen sind Vielfache dieses Theilers.

Beweis. Es mag α die kleinste unter den Zahlen sein, welche die Congruenz

$$a^x \equiv 1 \pmod{p}$$

befriedigen; dann wird, nach dem vorhergehenden Lehrsatze, dieselbe Congruenz auch durch den grössten gemeinsamen Theiler von α und $p-1$ befriedigt werden. Dieser Theiler von α und $p-1$, welcher die Congruenz

$$a^x \equiv 1 \pmod{p}$$

befriedigt, kann aber nur gleich α sein; da er sonst kleiner als α wäre, während nach der Voraussetzung α die kleinste unter den die Congruenz

$$a^x \equiv 1 \pmod{p}$$

befriedigenden Zahlen sein soll. Folglich muss α selbst ein Theiler von $p-1$ sein.

Wir wollen nun beweisen, dass alle Zahlen, welche die Congruenz

$$a^x \equiv 1 \pmod{p}$$

befriedigen, Vielfache von α sein müssen.

Zu diesem Zwecke bemerken wir, dass nach dem Vorhergehenden Lehrsatze zugleich mit der Congruenz

$$a^x \equiv 1 \pmod{p}$$

auch die Congruenz

$$a^\omega \equiv 1 \pmod{p}$$

bestehen muss, wobei ω den grössten gemeinsamen Theiler von x und $p-1$ bedeutet. Aus der letzten Congruenz, in Verbindung mit

$$a^\alpha \equiv 1 \pmod{p},$$

folgt aber, nach Lehrsatz 34, die neue Congruenz

$$a^{\omega'} \equiv 1 \pmod{p},$$

wobei ω' den grössten gemeinsamen Theiler von α und ω bedeutet. Es kann aber ω' nur gleich α sein; weil sonst ω', als grösster gemeinsamer Theiler von α und ω, kleiner als α wäre und wir hätten somit eine Zahl ω', welche kleiner als α wäre und die Congruenz

$$a^x \equiv 1 \pmod{p}$$

befriedigt; was der Voraussetzung, dass α die allerkleinste unter den diese Congruenz befriedigenden Zahlen sei, widerspricht. Es ist also

$$\omega' = \alpha.$$

Es war aber ω' der grösste gemeinsame Theiler von x und $p-1$; folglich muss $\alpha = \omega'$ ein Theiler einer jeden Zahl x sein, welche die genannte Congruenz befriedigt, was wir beweisen wollten.



Beispiel. Bemerkt man, dass, nach der Null, die 5 die kleinste Zahl ist, welche die Congruenz

$$2^x \equiv 1 \pmod{31}$$

befriedigt, so schliessen wir daraus, dass überhaupt nur Vielfache von 5 diese Congruenz befriedigen können.

Aus dem soeben bewiesenen Lehrsatze folgt, dass die *kleinste Zahl*, welche die Congruenz

$$a^x \equiv 1 \pmod{p}$$

befriedigt, einer von den Theilern von $p-1$ sein muss; $p-1$ selbst nicht ausgenommen, welche Zahl nach dem *Fermat*'schen Satze die Congruenz

$$a^{p-1} \equiv 1 \pmod{p}$$

befriedigt. Bezeichnen wir daher den kleinsten Divisor von $p-1$, welcher die Congruenz

$$a^x \equiv 1 \pmod{p}$$

befriedigt, mit α, so bilden alle Zahlen, welche überhaupt diese Congruenz befriedigen, die Reihe

$$0, \quad \alpha, \quad 2\alpha, \quad \ldots\ldots$$

Sollen aber die Zahlen, welche die Congruenz

$$a^x \equiv 1 \pmod{p}$$

befriedigen, noch der Bedingung unterliegen kleiner als $p-1$ zu sein, so können dieselben keine anderen sein, als die $\frac{p-1}{\alpha}$ folgenden:

$$0, \quad \alpha, \quad 2\alpha, \quad \ldots\ldots, \quad \alpha\left(\frac{p-1}{\alpha}-1\right).$$

Nach der oben für die Anzahl der Lösungen gegebenen Definition, sagen wir also:

die Congruenz

$$a^x \equiv 1 \pmod{p}$$

besitzt immer die $\frac{p-1}{\alpha}$ *Lösungen, welche durch*

$$x \equiv 0;\ x \equiv \alpha;\ x \equiv 2\alpha;\ \ldots;\ x \equiv \alpha\left(\frac{p-1}{\alpha}-1\right) \pmod{p-1}$$

dargestellt werden.

Beispiel. Haben wir bemerkt, dass die kleinste, von Null verschiedene Zahl, welche die Congruenz

$$2^x \equiv 1 \pmod{31}$$

befriedigt, 5 ist, so schliessen wir daraus, dass diese Congruenz

$$\frac{31-1}{5} = 6$$

Lösungen besitzt, welche durch

$$x \equiv 0;\ x \equiv 5;\ x \equiv 2.5;\ x \equiv 3.5;\ x \equiv 4.5;\ x \equiv 5.5 \pmod{30}$$

dargestellt sind.

Wir haben somit gefunden, dass die Anzahl der Lösungen der Congruenz

$$a^x \equiv 1 \pmod{p}$$

durch den Quotienten

$$\frac{p-1}{\alpha}$$

bestimmt ist, wobei α die kleinste von Null verschiedene Zahl bedeutet, welche überhaupt die Congruenz befriedigt. Daraus folgt, als specieller Fall:

die Congruenz $a^x \equiv 1 \pmod{p}$ hat nur eine einzige Lösung, wenn die kleinste sie befriedigende, von Null verschiedene, Zahl $p-1$ ist. Diese Lösung ist dann durch

$$x \equiv 0 \pmod{p-1}$$

dargestellt.

---

§ 35. Ueber die Lösungen der Congruenz
$a^x \equiv A \pmod{p}$.

Wir gehen nunmehr zu den allgemeineren Congruenzen

$$a^x \equiv A \pmod{p}$$

über, wobei A eine beliebige, durch p nicht theilbare Zahl ist, und beweisen folgenden Lehrsatz.

44. *Lehrsatz.* *Genügt der Congruenz*

$$a^x \equiv A \pmod{p}$$

eine Zahl λ, während α die kleinste Zahl ist, welche die Congruenz

$$a^x \equiv 1 \pmod{p}$$

befriedigt, so hat die erstere [ebenfalls]

$$\frac{p-1}{\alpha}$$

Lösungen, welche durch

$$x \equiv \lambda; \quad x \equiv \lambda + \alpha; \quad x \equiv \lambda + 2\alpha; \quad \ldots;$$
$$x \equiv \lambda + \left(\frac{p-1}{\alpha} - 1\right)\alpha \pmod{p-1}$$

dargestellt sind.

Beweis. Befriedigen λ und α beziehungsweise die Congruenzen

$$a^x \equiv A; \quad a^x \equiv 1 \pmod{p},$$

so hat man die beiden Congruenzen

$$a^\lambda \equiv A; \quad a^\alpha \equiv 1 \pmod{p}.$$

Erhebt man beide Seiten der zweiten dieser Congruenzen zu einer beliebigen, etwa n^{ten}, Potenz und multiplicirt das Resultat gliedweise mit der ersteren der beiden letzten Congruenzen, so erhält man

$$a^{\lambda+n\alpha} \equiv A \pmod{p},$$

woraus erhellt, dass $x = \lambda + n\alpha$ die Congruenz

$$a^x \equiv A \pmod{p}$$

befriedigt, wenn n eine beliebige ganze Zahl bedeutet.

Man kann sich aber auch leicht überzeugen, dass es ausser den Zahlen von der Form $\lambda + n\alpha$ keine sonst giebt, welche der Congruenz

$$a^x \equiv A \pmod{p}$$

Genüge leisten könnten.

Denn, da λ nach der Voraussetzung die Congruenz

$$a^x \equiv A \pmod{p}$$

befriedigen soll, so folgt aus dieser letzteren auch

$$a^x \equiv a^\lambda \pmod{p}.$$

Dividirt man beide Seiten durch a^λ, so erhält man

$$a^{x-\lambda} \equiv 1 \pmod{p},$$

was, nach dem 43. Lehrsatze, aussagt, dass $x-\lambda$ durch α theilbar ist. Bezeichnet man den Quotienten der Division von $x-\lambda$ durch α mit n, so erhält man $x-\lambda = n\alpha$, also $x = \lambda + n\alpha$.

Somit sind alle Zahlen, welche der Congruenz

$$a^x \equiv A \pmod{p}$$

genügen, durch die Form $x = \lambda + n\alpha$, in welcher n eine beliebige ganze Zahl ist, vollständig bestimmt. Ertheilt man n in dieser Form Werthe, welche nach Modul $\frac{p-1}{\alpha}$ einander congruent sind, so erhält man für x Zahlen, welche nach dem Modul $p-1$ einander congruent sind. Und umgekehrt: irgend zwei nach Modul $\frac{p-1}{\alpha}$ *incongruenten* Werthen von n entsprechen *incongruente* Werthe von $x = \lambda + n\alpha$. Davon überzeugen wir uns, indem wir bemerken, dass die Congruenz

$$\lambda + \alpha n \equiv \lambda + \alpha n' \pmod{p-1}$$

durch Subtraction von λ und Division beider Seiten und des Moduls durch α in

$$n \equiv n' \left(\text{mod.}\, \frac{p-1}{\alpha}\right)$$

übergeht.

Nach Modul $\frac{p-1}{\alpha}$ sind aber alle Zahlen überhaupt beziehungsweise congruent irgend einer von den untereinander *incongruenten* Zahlen

$$0,\ 1,\ 2,\ \ldots.,\ \frac{p-1}{\alpha}-1;$$

folglich sind alle durch die Form $x = \lambda + \alpha n$ bestimmten Zahlen irgend einer der Zahlen

$$\lambda,\ \ \lambda+\alpha;\ \ \lambda+2\alpha;\ \ \ldots.;\ \ \lambda+\alpha\left(\frac{p-1}{\alpha}-1\right)$$

nach dem Modul $p-1$ congruent, während diese Zahlen selbst einander *incongruent* sind.

Es werden daher alle Zahlen von der Form $\lambda + n\alpha$, d. h. alle die Congruenz

$$a^x \equiv A \pmod{p}$$

befriedigende Zahlen durch die Congruenzen

$$x \equiv \lambda;\ \ x \equiv \lambda+\alpha;\ \ x \equiv \lambda+2\alpha;\ \ldots.;\ x \equiv \lambda+\alpha\left(\frac{p-1}{\alpha}-1\right) \pmod{p-1},$$

welche sämmtlich von einander verschieden sind, vollständig bestimmt. Dadurch ist unser Lehrsatz bewiesen.

Beispiel. Bemerkt man, dass die Congruenz

$$2^x \equiv 13 \pmod{17}$$

durch $x = 6$ befriedigt wird, während 8 die kleinste Zahl ist, welche die Congruenz

$$2^x \equiv 1 \pmod{17}$$

befriedigt, so schliessen wir, dass die Congruenz

$$2^x \equiv 13 \pmod{17}$$

$\frac{17-1}{8} = 2$ Lösungen hat, welche durch die Congruenzen

$$x \equiv 6;\ \ x \equiv 6+8 \pmod{16}$$

dargestellt sind.

---

§ 36. Ueber die Indices.

Auf Grund des eben bewiesenen Lehrsatzes wird die Anzahl der Lösungen der Congruenz

$$a^x \equiv A \pmod{p},$$

falls dieselbe überhaupt möglich ist, durch die Anzahl der Lösungen der Congruenz

$$a^x \equiv 1 \pmod{p}$$

bestimmt. Wir wollen jetzt den speciellen Fall betrachten, wenn die Congruenz

$$a^x \equiv 1 \pmod{p}$$

eine einzige Lösung besitzt; d. h., wie wir wissen, wenn $p-1$ die kleinste Zahl ist, welche die letztgenannte Congruenz befriedigt.

In diesem Falle sagt man:

„die Zahl a sei primitive Wurzel der Primzahl p".

Die betreffende Congruenz

$$a^x \equiv A \pmod{p},$$

ist dann durch ihre eigenthümliche Eigenschaften und wegen ihrer Anwendbarkeit besonders bemerkenswerth. Mit dieser besondern Congruenz wollen wir uns jetzt beschäftigen und beweisen in Bezug auf dieselbe folgenden Lehrsatz.

45. *Lehrsatz. Ist a primitive Wurzel von p und A nicht durch p theilbar, so hat die Congruenz*

$$a^x \equiv A \pmod{p}$$

eine und nur eine Lösung.

Beweis. Nach der Beschaffenheit der primitiven Wurzel a, muss $p-1$ die kleinste Zahl sein, welche die Congruenz

$$a^x \equiv 1 \pmod{p}$$

befriedigt. In diesem Falle kann aber die Congruenz

$$a^x \equiv A \pmod{p},$$

nach dem vorhergehenden Lehrsatze, entweder *eine* Lösung besitzen, oder gar keine. Wir wollen nun beweisen, dass Letzteres unmöglich ist, sobald A durch p nicht theilbar sein soll.

Lassen wir nämlich, zu diesem Zwecke, zu, dass die Congruenz

$$a^x \equiv A \pmod{p}$$

keine Lösung besitzt, während A kein Vielfaches von p sein soll. Es muss dann die Division von A durch p eine der Zahlen

$$1, 2, \ldots, p-1$$

als Rest liefern; mit anderen Worten, es muss A einer dieser Zahlen nach dem Modul p congruent sein. Es mag r diese Zahl sein. Auf Grund von

$$A \equiv r \pmod{p}$$

können die beiden Congruenzen

$$a^x \equiv A \pmod{p} \quad \text{und} \quad a^x \equiv r \pmod{p}$$

nur gleichzeitig möglich, oder unmöglich sein. Da nun nach der Annahme

$$a^x \equiv A \pmod{p}$$

keine Lösung haben soll, so kann dann auch

$$a^x \equiv r \pmod{p}$$

keine Lösung besitzen.

Weil aber a relativ prim zu p ist, so können

$$a^0, \; a^1, \; a^2, \; \ldots, \; a^{p-2}$$

nicht durch p theilbar sein; es muss daher jede dieser Potenzen irgend einer der Zahlen

$$1, \; 2, \; 3, \; \ldots, \; p-1$$

nach Modul p congruent sein.

Daraus folgt, dass jede der $p-1$ Zahlen

$$0, \; 1, \; 2, \; \ldots, \; p-2$$

irgend einer der Congruenzen

$$a^x \equiv 1; \quad a^x \equiv 2; \quad a^x \equiv 3; \quad \ldots; \quad a^x \equiv p-1 \pmod{p}$$

genügen muss. Eine darunter ist aber die Congruenz

$$a^x \equiv r \pmod{p}$$

ist, welche keine Lösung haben soll, so müssen die $p-1$ Zahlen 0, 1, 2, ..., $p-2$ den übrigen $p-2$ Congruenzen genügen. Daraus folgt, dass mindestens eine dieser $p-2$ Congruenzen durch zwei von den Zahlen 0, 1, 2, ..., $p-2$ befriedigt werden müsste; was aber unmöglich ist, weil dieses heissen würde: eine dieser Congruenzen habe zwei Lösungen.

Es ist somit die Annahme, die Congruenz

$$a^x \equiv A \pmod{p}$$

habe gar keine Lösung, während A durch p nicht theilbar ist, unrichtig; und das war es ja, was wir beweisen wollten.

Aus diesem Lehrsatze schliessen wir, dass wenn a eine primitive Wurzel von p ist, die Congruenz

$$a^x \equiv A \pmod{p}$$

für jede durch p nicht theilbare Zahl A eine Lösung besitzt, d. h. diese Congruenz wird durch eine Zahl befriedigt, welche kleiner als $p-1$ und nicht kleiner als Null ist. Eine solche Zahl nennt man dann: *den Index der Zahl A;* die primitive Wurzel a nennt man in dieser Beziehung: *die Basis der Indices.*

Eine Zahl x wird somit *Index* einer Zahl A, in Bezug auf die Basis a sein, wenn x eine Zahl, welche kleiner als $p-1$ und nicht kleiner als Null ist und die Congruenz

$$a^x \equiv A \pmod{p}$$

befriedigt, während die kleinste Zahl, welche die Congruenz

$$a^x \equiv 1 \pmod{p}$$

befriedigt, $p-1$ ist. In diesem Falle schreibt man:

$$x = \text{Ind. } A.$$

Man findet somit Ind. A, indem man die Congruenz

$$a^x \equiv A \pmod{p}$$

löst und unter den Zahlen, welche dieselbe befriedigen,



diejenige nimmt, welche kleiner als $p-1$ und nicht kleiner als Null ist.

Wir werden also bei bestimmter Zahl a und bestimmtem Modul p für jede Zahl A eine gewisse zugehörige Zahl als Index von A finden.

Kennen wir umgekehrt

$$\text{Ind.}\, A = x,$$

so haben wir für die Bestimmung der Zahl A die Congruenz

$$a^x \equiv A \pmod{p}.$$

Dadurch wird aber die Zahl A noch nicht vollständig bestimmt, weil dieser Congruenz auch alle Zahlen, welche nach Modul p congruent A sind, ebenfalls genügen; *alle solche Zahlen haben somit einen und denselben Index.*

Indem uns also der Index einer Zahl A gegeben wird, erfahren wir nur eine Zahl, welcher A nach Modul p congruent ist; diese Zahl wird durch die Congruenz

$$A \equiv a^x \pmod{p} \text{ bestimmt, wenn } x = \text{Ind.}\, A$$

ist.

Beispiel. Es sei $p = 7$. Da die Congruenz

$$3^x \equiv 1 \pmod{7}$$

durch keine der Zahlen 1, 2, 3, 4, 5 befriedigt wird, so ist 3 primitive Wurzel von 7. Wir nehmen nun 3 zur Basis und finden dann die zugehörigen Indices der Zahlen

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,$$

und dieselben werden zugleich auch die Indices aller Zahlen sein, welche nach Modul 7 den erwähnten Zahlen

$$1,\ 2,\ 3,\ 4,\ 5,\ 6$$

congruent sind.

Um zunächst den Index von 1 zu finden, haben wir die Congruenz

$$3^x \equiv 1 \pmod{7}$$

zu lösen. Dieser Congruenz genügt offenbar $x = 0$;

folglich ist

$$\text{Ind. } 1 = 0.$$

Man überzeugt sich leicht, dass der Index von 1 *immer* 0 sein wird, weil die Congruenz

$$a^x \equiv 1 \pmod{p}$$

für irgend welche a und p immer durch

$$x = 0$$

befriedigt wird.

Um ferner die Indices der Zahlen

$$2, \ 3, \ 4, \ 5, \ 6$$

aufzufinden, haben wir die Congruenzen

$$3^x \equiv 2; \quad 3^x \equiv 3; \quad 3^x \equiv 4; \quad 3^x \equiv 5; \quad 3^x \equiv 6 \pmod{7}$$

zu lösen und unter den diese Congruenzen befriedigenden Zahlen diejenigen zu nehmen, welche kleiner als $7-1=6$ und nicht kleiner als Null sind. Dieses führt aber auf die Aufgabe, zu bestimmen, welche von den Zahleu

$$3^1, \ 3^2, \ 3^3, \ 3^4, \ 3^5$$

einer der Zahlen

$$2, \ 3, \ 4, \ 5, \ 6$$

nach Modul 7 congruent ist. Da nun diese successiven Potenzen beziehungsweise die Zahlen

$$3, \ 9, \ 27, \ 81, \ 243$$

liefern, die bei der Division durch 7 die entsprechenden Reste

$$3, \ 2, \ 6, \ 4, \ 5$$

ergeben, so erhalten wir

$$3^1 \equiv 3; \quad 3^2 \equiv 2; \quad 3^3 \equiv 6; \quad 3^4 \equiv 4; \quad 3^5 \equiv 5 \pmod{7}.$$

Es ergiebt sich somit:

$$\text{Ind. } 3 = 1; \ \text{Ind. } 2 = 2; \ \text{Ind. } 6 = 3; \ \text{Ind. } 4 = 4; \ \text{Ind. } 5 = 5.$$

Ordnet man diese Resultate nach den Zahlen, deren Indices gesucht werden, so erhält man die zugehörige Tabelle:

$$\text{Ind. } 1 = 0; \ \text{Ind. } 2 = 2; \ \text{Ind. } 3 = 1; \ \text{Ind. } 4 = 4;$$
$$\text{Ind. } 5 = 5; \ \text{Ind. } 6 = 3.$$

Aus dieser Tabelle finden wir die Indices irgend welcher Zahlen A, welche relativ prim zu 7 sind, indem wir überlegen, dass irgend eine solche Zahl je nachdem sie nach Modul 7 einer der Zahlen

$$1,\ 2,\ 3,\ 4,\ 5,\ 6$$

congruent ist, sie auch mit der entsprechenden dieser Zahlen gleichen Index haben wird. — Um z. B. die Indices von 20 und (—18) zu bestimmen, finden wir, dass diese Zahlen nach Modul 7 beziehungsweise den Zahlen 6, 3 congruent sind; daraus folgt:

$$\text{Ind. } 20 \quad = \text{Ind. } 6 = 3;$$
$$\text{Ind. } (-18) = \text{Ind. } 3 = 1.$$

Damit man die Zahlen aus ihren gegebenen Indices leichter finden kann, ordnen wir die obige Tabelle auch so:

$$0 = \text{Ind. } 1;\ \ 1 = \text{Ind. } 3;\ \ 2 = \text{Ind. } 2;\ \ 3 = \text{Ind. } 6;$$
$$4 = \text{Ind. } 4;\ \ 5 = \text{Ind. } 5.$$

Aus dieser Tabelle findet man leicht, welche von den Zahlen 1, 2, 3, 4, 5 einen gegebenen Index besitzt. So finden wir z. B. dass der Index 3 der Zahl 6 zugehört, woraus wir schliessen, dass alle Zahlen, welche in Bezug auf den Modul 7 und die Basis 3 den Index 3 besitzen, nach Modul 7 congruent 6 sind.

Aus der eben gegebenen Erläuterung erhellt, dass die Zusammenstellung solcher Tabellen gar keine weiteren Schwierigkeiten hat, sobald die primitiven Wurzeln gefunden sind. Wie man aber die primitiven Wurzeln finden kann, das werden wir weiter unten zeigen; hier dagegen wollen wir uns mit einer Auseinandersetzung einiger wichtigen Eigenschaften der Indices beschäftigen, welche es möglich machen, die betreffenden Tabellen mit sehr grossem Vortheil für die Lösung vieler Aufgaben der Zahlentheorie zu gebrauchen.

Am Schlusse dieses Buches findet man Tabellen, welche die Indices für alle Moduli, die kleiner als 200

sind, enthalten. Dieselben sind aus den Vorlesungen über algebraische und transcendente Analysis, des Herrn Ostrogradsky, Mitgliedes der Akademie der Wissenschaften, entlehnt.

Die Tabellen unter dem Buchstaben I (Index) dienen zur Bestimmung der Indices einer gegebenen Zahl; während die Tabellen unter dem Buchstaben N (Numerus) dazu dienen, aus gegebenem Index die betreffende Zahl zu finden. In den einen, wie in den anderen Tabellen wird die gegebene Zahl (gleichviel ob Index, oder Numerus) zerlegt in Einer und Zehner; die Einer findet man in der oberen Zeile und die Zehner in der äussersten linken Colonne und das Gesuchte (Numerus, oder Index) befindet sich in gleicher verticalen Colonne mit den Einern und gleicher horizontalen Zeile mit den Zehnern.

Um z. B. den Index von 167 in Bezug auf den Modul 193 zu finden, suchen wir in der mit I überschriebenen Tabelle für die Primzahl 193 in der oberen Zeile die Zahl 7 (die Einer von 167) und in der äusserst linken Colonne die Zahl 16 (die Zehner von 167) auf; auf gleicher Horizontalen mit 16 und gleicher Verticalen mit 7 findet man 101; diese ist der gesuchte Index von 167.

Wollen wir umgekehrt, bei demselben Modul und derselben Basis, diejenigen Zahlen finden, welche den Index 101 haben, so suchen wir in der mit N überschriebenen Tabelle in der oberen Zeile die Zahl 1 (Einer des Index 101) und in der äusserst linken Colonne die Zahl 10 (Zehner von 101) und finden 167 als entsprechenden Numerus in der Tabelle. Daraus schliessen wir, dass die Zahlen, welche den Index 101 haben nach Modul 193 congruent 167 sind.

---

§ 37. Ueber die Lösung binomischer Congruenzen mit Hülfe der Index-Tabellen.

Wir wollen uns jetzt mit denjenigen Eigenschaften der Indices beschäftigen, auf welchen der Gebrauch der Tabellen beruht.

46. *Lehrsatz.* *Für den Modul p ist der Index eines Productes mehrerer Zahlen congruent der Summe ihrer Indices nach Modul $p-1$.*

Beweis. Es mögen A, B, C, ... gegebene Zahlen und i, i', i'', ... ihre entsprechenden Indices in Bezug auf den Modul p und auf die Basis a sein. Nach der Definition des Index erhalten wir:

$$a^i \equiv A;\quad a^{i'} \equiv B;\quad a^{i''} \equiv C;\quad \ldots.;\quad (\text{mod.}\, p).$$

Multiplicirt man diese Congruenzen gliedweise mit einander, so findet man

$$a^{i+i'+i''+\cdots} \equiv A\,B\,C\ldots\ (\text{mod.}\, p).$$

Ist nun I der Index des Productes $ABC\ldots.$, so hat man

$$a^I \equiv A\,B\,C\ \ldots.\ (\text{mod.}\, p),$$

folglich, in Verbindung mit der vorhergehenden,

$$a^{i+i'+i''+\cdots} \equiv a^I\ (\text{mod.}\, p),$$

woraus nach Division durch a^I:

$$a^{i+i'+i''+\cdots-I} \equiv 1\ (\text{mod.}\, p).$$

Die Zahl

$$i+i'+i''+\ldots-I$$

genügt somit der Congruenz

$$a^x \equiv 1\ (\text{mod.}\, p),$$

was nach Lehrsatz 43 beweist, dass diese Zahl ein Vielfaches sein muss von derjenigen kleinsten Zahl, welche die letztgenannte Congruenz befriedigt; dieselbe kann nun, nach der Definition der primitiven Wurzel, keine andere als $p-1$ sein.

Die Differenz $i+i'+i''+\ldots-I$ ist also durch $p-1$ theilbar; diese Thatsache wird aber durch die Congruenz

$$I \equiv i+i'+i''+\ldots\ (\text{mod.}\, p-1)$$

ausgedrückt, was zu beweisen war.

Beispiel. In Bezug auf den Modul 199 und die Basis 127 finden wir:

$$\begin{aligned} \text{Ind. } 2 &= 194, \\ \text{Ind. } 5 &= 6, \\ \text{Ind. } 19 &= 11, \end{aligned}$$

folglich:

$$\text{Ind.}\, 2\,.\,5\,.\,19 = \text{Ind.}\, 190 \equiv 194 + 6 + 11; \ \text{Ind.}\, 190 \equiv 211 \pmod{198}.$$

Bemerken wir, dass die Zahl, welche kleiner als 198 und nach Modul 198 congruent 211 sein soll, 13 wird, so schliessen wir daraus, dass

$$\text{Ind.}\, 190 = 13$$

ist; welches sich auch in der Tabelle bestätigt findet.

Auf diese Weise kann man immer den Index einer zusammengesetzten Zahl finden, sobald die Indices ihrer Primzahl-Factoren gegeben sind.

Als speciellen Fall, finden wir in dem oben bewiesenen Lehrsatze noch folgenden

Zusatz. Der Index einer Potenz ist nach Modul $p-1$ dem Producte aus dem Exponenten und dem Index der Wurzel congruent.

Denn, nimmt man in der oben gefundenen Formel

$$\text{Ind.}\, A\,B\,C\, \ldots . \equiv \text{Ind.}\, A + \text{Ind.}\, B + \text{Ind.}\, C + \ldots . \pmod{p-1}$$

an, es sei n die Anzahl der darin auftretenden Zahlen A, B, C, ... und setzt $A = B = C = \ldots .$, so findet man:

$$\text{Ind.}\, A^n \equiv n \ \text{Ind.}\, A \pmod{p-1}.$$

Beispiel. In Bezug auf Modul 199 findet man:

$$\text{Ind.}\, 2^3 \equiv 3 \ \text{Ind.}\, 2 \pmod{198}.$$

Da nun Ind. 2 = 194 ist, so wird

$$\text{Ind.}\, 2^3 \equiv 3\,.\,194 \equiv 582 \pmod{198},$$



oder, wenn man die Zahl aufsucht, welche kleiner als 198 und nach Modul 198 congruent 582 ist,

$$\text{Ind.}\, 2^3 = 186,$$

wie man es auch durch die Tafel bestätigt findet.

---

47. *Lehrsatz.* *Befriedigt x die Congruenz*

$$Ax^n \equiv B \pmod{p},$$

wobei A und B durch p nicht theilbar sind, während p eine Primzahl ist, so befriedigt der Index von x die Congruenz

$$n\,.\text{Ind.}\,x \equiv \text{Ind.}\,B - \text{Ind.}\,A \pmod{p-1}.$$

Beweis. Da zwei Zahlen, welche nach Modul p einander congruent sind, in Bezug auf denselben Modul gleichen Index haben, so folgt aus der Congruenz

$$Ax^n \equiv B \pmod{p}$$

auch

$$\text{Ind.}\,(Ax^n) = \text{Ind.}\,B.$$

Nach obigem Lehrsatze ist aber

$$\text{Ind.}\,Ax^n \equiv \text{Ind.}\,A + \text{Ind.}\,x^n \pmod{p-1}$$

und

$$\text{Ind.}\,x^n \equiv n\,.\,\text{Ind.}\,x \pmod{p-1},$$

folglich ist:

$$\text{Ind.}\,A + n\,.\,\text{Ind.}\,x \equiv \text{Ind.}\,B \pmod{p-1},$$

woraus sich

$$n\ \text{Ind.}\,x \equiv \text{Ind.}\,B - \text{Ind.}\,A \pmod{p-1}$$

ergiebt, w. z. b. w.

Auf Grund dieses Lehrsatzes kann man leicht alle Congruenzen von der Form

$$Ax^n \equiv B \pmod{p}$$

lösen, wenn p Primzahl ist und A, wie B durch p nicht theilbar.

Dahin gehören, als specielle Fälle, alle Congruenzen ersten Grades (für $n = 1$); die Congruenz zweiten Grades

$$x^2 \equiv q \pmod{p}$$

(für $n = 2$ und $A = 1$; $B = q$) und alle binomische Congruenzen.

Wir beginnen mit der Anwendung des Lehrsatzes auf die Lösung der Congruenzen ersten Grades.

Lautet die gegebene Congruenz

$$Ax \equiv B \pmod{p},$$

so hat man nach dem vorhergehenden Lehrsatze:

$$\text{Ind.}\, x \equiv \text{Ind.}\, B - \text{Ind.}\, A \pmod{p-1}.$$

Da nun der Index von x nicht kleiner als Null und nicht grösser als $p-2$ sein kann, so finden wir aus dieser Congruenz für Ind. x einen bestimmten Werth, indem man die kleinste positive Zahl aufsucht, welche der Zahl Ind. B — Ind. A nach Modul $p-1$ congruent ist. Haben wir nun den Ind. von x gefunden, so werden wir in der Tabelle eine Zahl (Numerus) finden, welcher x nach Modul p congruent ist und dieses wird eben die gesuchtste Lösung der Congruenz

$$Ax \equiv B \pmod{p}$$

sein.

Beispiel. Um die Lösung der Congruenz

$$10\,x \equiv 9 \pmod{11}$$

zu finden, haben wir:

$$\text{Ind.}\, x \equiv \text{Ind.}\, 9 - \text{Ind.}\, 10 \pmod{10}.$$

In der zur Primzahl 11 gehörigen Tabelle finden wir:

$$\text{Ind.}\, 9 = 6,$$
$$\underline{\text{Ind.}\, 10 = 5,}$$

also $\text{Ind.}\, 9 - \text{Ind.}\, 10 = 1$; folglich ist

$$\text{Ind.}\, x \equiv 1 \pmod{10}$$

und mithin auch bestimmter:

$$\text{Ind.}\, x = 1.$$

In der entsprechenden Tabelle für den Numerus findet

man, dass dem Index 1 der Numerus 2 entspricht; dem Ind. $x = 1$ entspricht also $x = 2$, folglich ist

$$x \equiv 2 \pmod{11}$$

die Lösung der Congruenz

$$10\,x \equiv 9 \pmod{11}.$$

Was nun die Lösung der Congruenz zweiten Grades von der Form

$$x^2 \equiv q \pmod{p}$$

betrifft, so erhält man nach der obigen allgemeinen Formel

$$2 \,.\, \text{Ind.}\, x \equiv \text{Ind.}\, q \pmod{p-1}.$$

Nehmen wir hier an, es sei p ungerade, so bemerken wir, dass der Coefficient von Ind. x und der Modul durch 2 theilbar sind; daraus schliessen wir, auf Grund des Lehrsatzes 18, dass die Congruenz

$$2 \,.\, \text{Ind.}\, x \equiv \text{Ind.}\, q \pmod{p}$$

und somit auch die Congruenz

$$x^2 \equiv q \pmod{p}$$

überhaupt keine Lösung haben kann, wenn q durch 2 nicht theilbar ist.

Im entgegengesetzten Falle wird die Congruenz

$$2 \,.\, \text{Ind.}\, x \equiv \text{Ind.}\, q \pmod{p-1}$$

nach Lehrsatz 19 zwei Lösungen haben; es werden sich also 2 Zahlen in der Reihe

$$0,\ 1,\ 2,\ \ldots,\ p-2,$$

finden, welche der Congruenz genügen. Diese Zahlen werden dann die Werthe von Ind. x sein und ihnen entsprechen zwei Lösungen der Congruenz

$$x^2 \equiv q \pmod{p}.$$

Beispiel. 1) Wir wollen die Lösungen der Congruenz

$$x^2 \equiv 10 \pmod{101}$$

aufsuchen. Dazu haben wir die Lösungen von

$$2 \,.\, \text{Ind.}\, x \equiv \text{Ind.}\, 10 \pmod{100}$$

aufzufinden. Nach der Tabelle finden wir

$$\text{Ind.}\, 10 = 25,$$

also durch 2 nicht theilbar. Die Congruenz hat somit keine Lösung.

Sucht man den Werth des *Legender*'schen Symbols $\left(\frac{10}{101}\right)$ zu bestimmen, so findet man in der That:

$$\left(\frac{10}{101}\right) = \left(\frac{2}{101}\right)\left(\frac{5}{101}\right) = -\left(\frac{5}{101}\right) = -\left(\frac{101}{5}\right) = -\left(\frac{1}{5}\right) = -1,$$

woraus die Unmöglichkeit der Congruenz

$$x^2 \equiv 10 \pmod{101}$$

erhellt.

---

2) Es sei die Congruenz

$$x^2 \equiv 30 \pmod{107}$$

gegeben. Die Lösung dieser Congruenz wird auf die von

$$2\, \text{Ind.}\, x \equiv \text{Ind.}\, 30 \pmod{106}$$

zurückgeführt.

Nach der zur Primzahl 107 zugehörigen Tabelle ist

$$\text{Ind.}\, 30 = 80,$$

also eine gerade Zahl; folglich hat die Congruenz zwei Lösungen.

Indem man nun findet, dass die kleinsten Zahlen, welche die Congruenz

$$2 \,.\, \text{Ind.}\, x \equiv 80 \pmod{106}$$

befriedigen 40 und 93 sind, erhalten wir die zwei Werthe

$$\text{Ind.}\, x = 40 \text{ und } \text{Ind.}\, x = 93.$$

Diese Indices entsprechen aber den Zahlen

64 und 43,

folglich sind

$$x \equiv 64; \quad x \equiv 43 \pmod{107}$$

die Lösungen der Congruenz

$$x^2 \equiv 30 \pmod{107}.$$

Wir wenden uns endlich zur Lösung der binomischen Congruenzen von der Form

$$x^n \equiv B \pmod{p}.$$

Nach dem vorhergehenden Lehrsatze wird die Lösung dieser Congruenz auf die Congruenz

$$n \,\mathrm{Ind.}\, x \equiv \mathrm{Ind.}\, B \pmod{p-1}$$

zurückgeführt.

Nach Lehrsatz 18 ist die letzte Congruenz unmöglich, wenn der grösste gemeinsame Theiler von n und $p-1$ kein Theiler von Ind. B ist; in diesem Falle hat also auch die Congruenz

$$x^n \equiv B \pmod{p}$$

keine Lösung.

Ist dagegen der grösste gemeinsame Theiler von n und $p-1$, welcher mit ω bezeichnet werden möge, auch ein Theiler von Ind. B, so hat die Congruenz

$$n \,.\, \mathrm{Ind.}\, x \equiv \mathrm{Ind.}\, B \pmod{p-1},$$

nach Lehrsatz 19, ω Lösungen. Daraus erhält man dann ω verschiedene Werthe von Ind. x und somit auch ω Lösungen der Congruenz

$$x^n \equiv B \pmod{p}.$$

Dieses alles wird auch durch Lehrsatz 38 bestätigt, nach welchem eine Congruenz von der Form

$$x^n \equiv B \pmod{p}$$

entweder gar keine Lösung besitzt, oder sie besitzt so viele Lösungen, als Einheiten in dem grössten gemeinsamen Theiler von n und $p-1$ vorhanden sind.

Beispiele. 1) Es sei gegeben die Congruenz

$$x^{12} \equiv 17 \pmod{127}.$$

Wir leiten aus dieser Congruenz folgende:

$$12 \,.\, \text{Ind.}\, x \equiv \text{Ind.}\, 17 \pmod{126}$$

her und suchen in der zur Primzahl 127 gehörigen Tabelle den Index von 17 auf.

Indem wir nun finden:

$$\text{Ind.}\, 17 = 118$$

und da 118 durch den grössten gemeinsamen Theiler von 12 und 126, nämlich durch 6 nicht theilbar ist, überzeugen wir uns, dass die Congruenz

$$12\, \text{Ind.}\, x \equiv \text{Ind.}\, 17 \pmod{126}$$

und somit auch die Congruenz

$$x^{12} \equiv 17 \pmod{127}$$

keine Lösung hat.

---

2) Es sei die Congruenz

$$x^{12} \equiv 38 \pmod{127}$$

gegeben. Aus dieser Congruenz erhalten wir

$$12\, \text{Ind.}\, x \equiv \text{Ind.}\, 38 \pmod{126}.$$

In derselben Tabelle, wie im vorigen Beispiel, finden wir

$$\text{Ind.}\, 38 = 60.$$

Da nun 60 durch den grössten gemeinsamen Theiler 6 von 12 und 126 theilbar ist, so hat die Congruenz

$$12\, \text{Ind.}\, x \equiv 60 \pmod{126}$$

6 Lösungen. Diese Lösungen finden wir nach Lehrsatz 19, indem wir beide Seiten und den Modul der letzten Congruenz durch 6 dividiren. Dadurch erhalten wir:

$$2\, \text{Ind.}\, x \equiv 10 \pmod{21}.$$

Wir finden aber, dass 5 die kleinste Zahl ist, welche dieser Congruenz genügt. Daraus ergeben sich die 6 Lösungen der Congruenz

$$12\, \text{Ind.}\, x \equiv 60 \pmod{126}$$

in der Gestalt:

$$\text{Ind.}\, x \equiv 5;\ \ \text{Ind.}\, x \equiv 26;\ \ \text{Ind.}\, x \equiv 47;\ \ \text{Ind.}\, x \equiv 68;$$
$$\text{Ind.}\, x \equiv 89;\ \ \text{Ind.}\, x \equiv 110 \pmod{126}.$$

Aus diesen Congruenzen ergeben sich folgende 6 Werthe für Ind. x, nämlich:

$$\text{Ind.}\, x = 5;\ \ 26;\ \ 47;\ \ 68;\ \ 89;\ \ 110$$

und diesen Werthen von Ind. x entsprechen in der zugehörigen Tabelle die Numeri

$$x = 65;\ \ 30;\ \ 92;\ \ 62;\ \ 97;\ \ 35.$$

Folglich sind

$$x \equiv 65;\ \ x \equiv 30;\ \ x \equiv 92;\ \ x \equiv 62;\ \ x \equiv 97;\ \ x \equiv 35 \pmod{127}$$

die Lösungen der Congruenz

$$x^{12} \equiv 17 \pmod{127}.$$

---

§ 38. Eigenschaften der primitiven Wurzeln.

Wir gehen jetzt zu der Bestimmung der primitiven Wurzeln über und wollen zunächst den Hilfssatz beweisen.

Hilfssatz. Jede zu p relative Primzahl a, die keiner der Congruenzen

$$\left.\begin{aligned} a^{\frac{p-1}{\alpha}} &\equiv 1 \\ a^{\frac{p-1}{\beta}} &\equiv 1 \\ a^{\frac{p-1}{\gamma}} &\equiv 1 \\ &\vdots \end{aligned}\right\} \pmod{p}$$

genügt, wenn $\alpha, \beta, \gamma, \ldots.$ die in $p-1$ enthaltenen Primzahlfactoren bedeuten, ist primitive Wurzel von p.

Denn, nach der oben gegebenen Definition, ist eine Zahl a primitive Wurzel von p, wenn der Congruenz

$$a^x \equiv 1 \pmod{p}$$

keine kleinere Zahl als $p-1$ genügt. Wir wollen nun

beweisen, dass dieses unter unseren gemachten Voraussetzungen wirklich der Fall ist. Zu diesem Zwecke wollen wir das Gegentheil zulassen und zeigen, dass eine solche Zulassung auf einen Widerspruch führt.

Wird die Congruenz

$$a^x \equiv 1 \pmod{p}$$

durch eine Zahl $x < p-1$ befriedigt, so wird nach Lehrsatz 42 auch die Congruenz

$$a^\omega \equiv 1 \pmod{p}$$

stattfinden, wobei ω den grössten gemeinsamen Theiler von x und $p-1$ bedeutet, so dass jedenfalls $\omega < p-1$ ist. Der Bruch $\frac{p-1}{\omega}$ wird dann eine ganze Zahl sein, welche 1 übertrifft. Diese Zahl kann aber nur diejenigen Primzahlfactoren $\alpha, \beta, \gamma, \ldots.$ enthalten, welche in $p-1$ enthalten sind. Folglich muss eine der Primzahlen $\alpha, \beta, \gamma, \ldots.$ ein Theiler des Quotienten $\frac{p-1}{\omega}$ sein; mag diese Primzahl β sein und der Quotient der Division von $\frac{p-1}{\omega}$ durch β mag mit ϱ bezeichnet werden. Aus $\frac{p-1}{\omega\beta} = \varrho$ erhalten wir:

$$\omega\varrho = \frac{p-1}{\beta}.$$

Erhebt man nun beide Seiten der Congruenz

$$a^\omega \equiv 1 \pmod{p}$$

zur ϱ^{ten} Potenz und setzt für $\omega\varrho$ seinen aus der letzten Gleichung erhaltenen Werth, so erhält man:

$$a^{\frac{p-1}{\omega}} \equiv 1 \pmod{p},$$

was der Voraussetzung widerspricht.

Es kann somit keine Zahl $x < p-1$ die Congruenz

$$a^x \equiv 1 \pmod{p}$$

befriedigen; es ist daher a eine primitive Wurzel von p, was wir beweisen wollten.

Auf Grund dieses Hilfssatzes, beweisen wir folgenden Lehrsatz.

48. *Lehrsatz.* *Besteht für a keine der Congruenzen*

$$x^\alpha \equiv a; \;\; x^\beta \equiv a; \;\; x^\gamma \equiv a; \;\ldots\ldots \pmod{p},$$

wenn $\alpha, \beta, \gamma, \ldots\ldots$ in $p-1$ enthaltene Primzahlfactoren bedeuten, so ist a primitive Wurzel von p; im entgegengesetzten Falle ist a keine primitive Wurzel.

Beweis. Nach Lehrsatz 38 folgt aus der Unmöglichkeit der Congruenzen

$$x^\alpha \equiv a, \;\; x^\beta \equiv a; \;\; x^\gamma \equiv a, \;\ldots\ldots \pmod{p},$$

wenn die Primzahlen $\alpha, \beta, \gamma, \ldots\ldots$ Theiler von $p-1$ sind, dass keine der Congruenzen

$$a^{\frac{p-1}{\alpha}} \equiv 1; \;\; a^{\frac{p-1}{\beta}} \equiv 1; \;\; a^{\frac{p-1}{\gamma}} \equiv 1; \;\ldots\ldots \pmod{p}$$

eine Lösung besitzen kann. In diesem Falle ist aber a, nach dem vorhergehenden Hilfssatze, eine primitive Wurzel der Zahl p.

Im entgegengesetzten Falle, wenn irgend eine der Congruenzen

$$x^\alpha \equiv a; \;\; x^\beta \equiv a; \;\; x^\gamma \equiv a; \;\ldots\ldots \pmod{p}$$

stattfindet, so wird auch eine der Congruenzen

$$a^{\frac{p-1}{\alpha}} \equiv 1; \;\; a^{\frac{p-1}{\beta}} \equiv 1; \;\; a^{\frac{p-1}{\gamma}} \equiv 1; \;\ldots\ldots \pmod{p}$$

stattfinden und die Zahl a ist daher keine primitive Wurzel.

---

§ 39. Ueber die Auffindung der primitiven Wurzeln.

Auf Grund des vorhergehenden Lehrsatzes können wir nun leicht alle diejenigen Zahlen aus der Reihe

$$1, \; 2, \; 3, \; \ldots\ldots, \; p-1$$

bestimmen, welche keine primitiven Wurzeln sind. Es ist nämlich, wie wir gesehen haben, a dann und nur dann

keine primitive Wurzel von p, wenn irgend eine der Congruenzen

$$x^\alpha \equiv a; \quad x^\beta \equiv a; \quad x^\gamma \equiv a; \quad \ldots . \pmod{p}$$

eine Lösung besitzt. Dieses heisst aber mit anderen Worten, wenn eine der Congruenzen

$$\left.\begin{array}{llll} 1^\alpha \equiv a; & 2^\alpha \equiv a; & 3^\alpha \equiv a; \; \ldots .; & (p-1)^\alpha \equiv a \\ 1^\beta \equiv a; & 2^\beta \equiv a; & 3^\beta \equiv a; \; \ldots .; & (p-1)^\beta \equiv a \\ 1^\gamma \equiv a; & 2^\gamma \equiv a; & 3^\gamma \equiv a; \; \ldots .; & (p-1)^\gamma \equiv a \\ \ldots & \ldots & \ldots & \ldots \end{array}\right\} \pmod{p}$$

befriedigt wird. Folglich erkennen wir, dass a dann und nur dann keine primitive Wurzel sein wird, wenn a einer Zahlen

$$\begin{array}{l} 1^\alpha; \; 2^\alpha; \; 3^\alpha; \; \ldots .; \; (p-1)^\alpha; \\ 1^\beta; \; 2^\beta; \; 3^\beta; \; \ldots .; \; (p-1)^\beta; \\ 1^\gamma; \; 2^\gamma; \; 3^\gamma; \; \ldots .; \; (p-1)^\gamma; \\ \ldots \ldots \ldots \end{array}$$

nach Modul p congruent ist.

Unter den Resten, welche die Division dieser Zahlen durch p ergiebt, findet man daher *alle* diejenigen Zahlen, welche kleiner als p und keine primitiven Wurzeln von p sind. *Lässt man diese Zahlen in der Reihe*

$$1, 2, 3, \ldots ., p-1$$

weg, so erhält man alle diejenigen primitiven Wurzeln von p welche kleiner als p sind.

Was nun die Zahlen betrifft, welche *grösser* als p sind und die Eigenschaft der primitiven Wurzel haben, so ist es leicht einzusehen, dass dieselben den ebengefundenen nach dem Modul p congruent sein werden; und wir werden uns daher dabei nicht weiter aufhalten, weil diese übrigen Zahlen uns kein besonderes Interesse bieten.

Und so werden wir, indem wir von der Anzahl der primitiven Wurzeln von p sprechen, immer nur diejenigen darunter verstehen, welche kleiner als p sind.

Beispiel. Wir wollen die eben auseinandergesetzte Methode auf die Aufsuchung aller primitiven Wurzeln der Primzahl 13 anwenden.

Da in $13-1$ die Primzahlfactoren 2 und 3 enthalten sind, so werden unter den Zahlen der Reihe

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$$

alle diejenigen, welche nicht bei der Division der Zahlen

$$1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2, 11^2, 12^2,$$
$$1^3, 2^3, 3^3, 4^3, 5^3, 6^3, 7^3, 8^3, 9^3, 10^3, 11^3, 12^3$$

durch 13 als Rest sich ergeben, primitive Wurzeln von 13 sein.

Die Division von

$$1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2, 11^2, 12^2$$

durch 13 liefert nun beziehungsweise folgende Reste:

$$1, 4, 9, 3, 12, 10, 10, 12, 3, 9, 4, 1,$$

während aus der Division von

$$1^3, 2^3, 3^3, 4^3, 5^3, 6^3, 7^3, 8^3, 9^3, 10^3, 11^3, 12^3$$

durch 13 sich beziehungsweise die Reste

$$1, 8, 1, 12, 8, 8, 5, 5, 1, 12, 5, 12$$

ergeben. Lässt man nun in der Reihe

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$$

alle die gefundenen Reste

$$1, \quad 3, 4, 5, \quad 8, 9, 10, \quad 12$$

weg, so verbleiben die Zahlen

$$2, 6, 7, 11$$

als primitive Wurzeln von 13.

---

§ 40. **Zweite Methode zur Auffindung der primitiven Wurzeln.**

Die im vorigen Paragraphen gegebene Methode zur Auffindung der primitiven Wurzeln, welche dadurch besonders bemerkenswerth ist, dass sie *alle* primitive Wurzeln zugleich liefert, wird practisch fast unausführbar,

sobald man die primitiven Wurzeln einer bedeutend grossen Zahl sucht. In diesem Falle pflegt es leichter zu sein, *eine* primitive Wurzel ausfindig zu machen (was für unseren Zweck, wie wir sehen werden, vollständig hinreicht) und zwar dadurch, dass man verschiedene Zahlen zu potenziren versucht, um diejenige ausfindig zu machen, die nach dem Modul p, in Bezug auf welchen wir eben die primitive Wurzel suchen, der 1 congruent ist.

Wenn wir bei der successiven Erhebung einer Zahl a zu den Potenzen 1, 2, 3, ... bis zu a^{p-1} gelangen, ohne darunter eine zu finden, welche nach dem Modul p congruent 1 wäre, so erhalten wir in a eine primitive Wurzel von p. Finden wir dagegen, dass

$$a^n \equiv 1 \pmod{p}$$

ist für $n < p-1$, so überzeugen wir uns, dass a keine primitive Wurzel ist. In dem letzteren Falle suchen wir dann eine Zahl, deren niedrigste Potenz, welche nach Modul p congruent 1 ist, grösser als n wird. Eine solche Zahl können wir aber immer finden, indem wir in folgender Weise verfahren.

Wir greifen aus der Reihe

$$1, 2, 3, \ldots, p-1$$

eine solche Zahl heraus, welche von den Resten der Division von

$$a^1, a^2, a^3, \ldots, a^n$$

durch p verschieden ist und suchen die niedrigste Potenz dieser Zahl auf, welche nach Modul p der Einheit congruent ist.

Es mag die von uns gewählte Zahl b sein und ihre niedrigste Potenz, welche nach dem Modul p congruent 1 wird, sei die m^{te}. Man kann sich leicht überzeugen, dass m weder gleich n, noch ein Theiler von n sein kann. Denn in jedem dieser Fälle würde die Zahl b die Congruenz

$$b^n \equiv 1 \pmod{p}$$

befriedigen, was nach dem 37ten Lehrsatze nicht möglich ist, wenn b^n nach Modul p nicht einer der Zahlen

$$a^1,\ a^2,\ \ldots.,\ a^{n-1}$$

congruent wäre, während n die kleinste Zahl bedeutet, welche die Congruenz

$$a^x \equiv 1 \pmod{p}$$

befriedigt. Daher muss m, *entweder* grösser als n sein und somit b dann eben die gesuchte Zahl sein wird, deren niedrigste Potenz, welche congruent 1 ist, n übertrifft, *oder* m enthält, falls $m < n$, einen Factor, welcher kein Theiler von n ist. Im letzteren Falle können wir vermittelst der Zahlen

$$a,\ b,\ m,\ n$$

leicht eine Zahl finden, deren niedrigste Potenz, welche congruent 1 wird, grösser als n ist.

Zu diesem Zwecke suchen wir den grössten gemeinsamen Theiler ω von m und n auf und zerlegen denselben so in zwei Factoren π und ϱ, dass die Zahlen

$$\frac{n}{\pi} \text{ und } \frac{m}{\varrho}$$

zu einander relativ prim werden(*). Nehmen wir dann die Zahl $a^\pi\, b^\varrho$, oder eine ihr nach Modul p congruente Zahl, so wird dieselbe so beschaffen sein, dass die niedrigste Potenz derselben, welche congruent 1 wird, grösser als n ist. Um uns davon zu überzeugen, wollen wir beweisen, dass wenn

$$c \equiv a^\pi\, b^\varrho; \quad c^N \equiv 1 \pmod{p}$$

ist, dann $\frac{nm}{\pi\varrho}$ ein Theiler von N sein muss; dadurch wird

---

(*) Um eine solche Zerlegung des grössten gemeinsamen Theilers ω zweier Zahlen m und n zu erwirken, zerlegen wir zunächst ω in seine Primzahlfactoren und nehmen für π diejenigen Primzahlfactoren, deren Exponenten in ω nicht niedriger, als die betreffenden in n sind; ganz analog nehmen wir für ϱ diejenigen Primzahlfactoren, deren Exponenten in ω nicht niedriger sind, als die entsprechenden in m. Was nun die Primzahlfactoren betrifft, deren Exponenten in m sowohl, als in n, und somit auch in ω, dieselben sind, so bleibt es ganz gleichgültig, ob man dieselben in π oder in ϱ aufnimmt.

bewiesen sein, dass die niedrigste Potenz N von c, welche congruent 1 wird, wirklich grösser als n ist. Denn $\pi\varrho = \omega$ muss, als gemeinsamer Theiler von m und n, wobei m kein Theiler von n ist, jedenfalls kleiner als m sein, folglich wird $n \cdot \frac{m}{\pi\varrho} > n$ und umsomehr $N > n$, wenn $\frac{nm}{\pi\varrho}$ ein Theiler von N sein soll.

Um nun zu beweisen, dass N durch $\frac{mn}{\pi\varrho}$ theilbar ist, sobald

$$c^N \equiv 1; \quad c \equiv a^\pi b^\varrho \pmod{p},$$

bemerken wir, dass die Elimination von c aus diesen beiden Congruenzen die Congruenz

$$a^{\pi N} b^{\varrho N} \equiv 1 \pmod{p}$$

ergiebt. Erhebt man jene Congruenzen zu den Potenzen $\frac{n}{\pi}$ und $\frac{m}{\varrho}$, so erhält man:

$$a^{nN} b^{\frac{\varrho n}{\pi} N} \equiv 1; \quad a^{\frac{m\pi}{\varrho} N} b^{mN} \equiv 1 \pmod{p}.$$

Wir wissen aber, dass m und n die Congruenzen

$$a^n \equiv 1; \quad b^m \equiv 1 \pmod{p}$$

befriedigen; die Verbindung dieser letzteren mit den vorhergehenden Congruenzen ergiebt daher

$$b^{\frac{n\varrho}{\pi} N} \equiv 1; \quad a^{\frac{m\pi}{\varrho} N} \equiv 1 \pmod{p}.$$

Aus diesen beiden Congruenzen kann man nach Lehrsatz 43 schliessen, dass $\frac{n\varrho}{\pi} N$ durch m theilbar ist und ebenso, dass $\frac{m\pi}{\varrho} N$ durch n theilbar sein muss; weil n und m als die kleinsten Zahlen vorausgesetzt waren, welche beziehungsweise den Congruenzen

$$a^x \equiv 1; \quad b^x \equiv 1 \pmod{p}$$

Genüge leisten. Die Theilbarkeit von $\frac{n\varrho}{\pi} N$ durch m und $\frac{m\pi}{\varrho} N$ durch n setzt aber voraus, dass

$$\frac{n\varrho N}{m\pi} \text{ und } \frac{m\pi N}{n\varrho}, \text{ oder } \frac{N\frac{n}{\pi}}{\frac{m}{\varrho}} \text{ und } \frac{N\frac{m}{\varrho}}{\frac{n}{\pi}}$$

ganze Zahlen seien. Es muss also die Zahl $N\frac{n}{\pi}$ durch $\frac{m}{\varrho}$ und zugleich $N\frac{m}{\varrho}$ durch $\frac{n}{\pi}$ theilbar sein, während $\frac{n}{\pi}$ und $\frac{m}{\varrho}$ relativ prim zu einander sind. Es ist dieses daher nur möglich, wenn N sowohl durch $\frac{m}{\varrho}$, als auch durch $\frac{n}{\pi}$ theilbar ist und folglich auch durch das Product $\frac{mn}{\varrho\pi}$, was wir zu beweisen hatten.

Zu einer Zahl, deren niedrigste Potenz, welche nach Modul p congruent 1 wird, n ist, während $n < p-1$, können wir also immer eine solche Zahl ausfindig machen, deren niedrigste Potenz, welche congruent 1 wird, grösser als n ist. Wiederholen wir nun das angegebene Verfahren eine genügende Anzahl mal, so müssen wir endlich (jedenfalls nach einer endlichen Anzahl von Wiederholungen) zu einer Zahl gelangen, deren niedrigste Potenz, welche nach Modul p congruent 1 ist, nicht kleiner als $p-1$ sein wird. Eine solche Zahl wird eben eine primitive Wurzel der Zahl p sein.

Beispiele. 1) Wir wollen nach dieser Methode eine primitive Wurzel der Primzahl 17 aufsuchen.

Wir versuchen zuerst, ob nicht die Zahl 2 (die kleinste, welche wir nehmen können) primitive Wurzel von 17 ist. Dividiren wir

$$2,\ 2^2,\ 2^3,\ 2^4,\ 2^5,\ 2^6,\ 2^7,\ 2^8,\ \ldots$$

durch 17, so erhalten wir die zugehörigen Reste

$$2,\ 4,\ 8,\ 16,\ 15,\ 13,\ 9,\ 1,\ \ldots$$

Indem wir so bereits bei der Division von 2^8 durch 17 zum Reste 1 gelangen, brechen wir, in der Ueberzeugung, dass 2 keine primitive Wurzel von 17 ist, die Divisionen hiermit ab. Darauf nehmen wir eine andere Zahl,

welche kleiner als 17 und nicht unter den früher gefundenen Resten

$$2, 4, 8, 16, 15, 13, 9$$

enthalten ist und probieren ob nicht diese primitive Wurzel sei. Die kleinste der möglichen Zahlen ist 3 und indem wir die successiven Potenzen von 3

$$3, 3^2, 3^3, 3^4, 3^5, 3^6, 3^7, 3^8, 3^9, 3^{10}, 3^{11}, 3^{12}, 3^{13}, 3^{14}, 3^{15}$$

durch 17 dividiren und die zugehörigen Reste

$$3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6$$

finden, überzeugen wir uns, dass 3, erst zur 16ten Potenz erhoben, nach Modul 17 congruent 1 wird und somit 3 wirklich eine primitive Wurzel von 17 ist.

---

2) Als zweites Beispiel wählen wir die Primzahl 73, um eine primitive Wurzel derselben ausfindig zu machen. Wir fangen wiederum das Probieren mit der kleinsten Zahl 2 an. Indem wir nun die successiven Potenzen

$$2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, \ldots$$

durch 73 dividiren und die zugehörigen Reste

$$2, 4, 8, 16, 32, 64, 55, 37, 1$$

finden, überzeugen wir uns, dass bereits 2^9 congruent 1 nach Modul 73 wird und somit 2 keine primitive Wurzel von 73 ist.

Indem wir nun bemerken, dass unter den erhaltenen Resten

$$2, 4, 8, 16, 32, 64, 55, 37$$

sich die nach 2 kleinste Zahl 3 nicht befindet, so nehmen wir jetzt das Probieren mit der Zahl 3 vor. Die Division von

$$3, 3^2, 3^3, 3^4, 3^5, 3^6, 3^7, 3^8, 3^9, 3^{10}, 3^{11}, 3^{12}, \ldots$$

durch 73 ergiebt die Reste

$$3, 9, 27, 8, 24, 72, 70, 64, 46, 65, 49, 1, \ldots$$

und zeigt somit, dass bereits



$$3^{12} \equiv 1 \pmod{73}$$

und folglich auch 3 keine primitive Wurzel von 73 ist.

Da aber die Zahlen 2 und 3 die Congruenzen

$$2^9 \equiv 1; \quad 3^{12} \equiv 1 \pmod{73}$$

ergeben, so können wir nach der oben auseinandergesetzten Methode leicht eine Zahl componiren, deren niedrigste Potenz, welche nach Modul 73 congruent 1 wird, jedenfalls grösser als 12 sein muss.

Zu diesem Zwecke bemerken wir, dass der grösste gemeinsame Theiler von 9 und 12 die Primzahl 3 ist, welche in 12 in erster Potenz und in 9 in zweiter Potenz enthalten ist. Um daher die Zerlegung von 3 in zwei Factoren π und ϱ so zu bewirken, dass

$$\frac{9}{\pi} \quad \text{und} \quad \frac{12}{\varrho}$$

relativ prim zu einander werden, nehmen wir $\pi = 1$; $\varrho = 3$. Es wird infolgedessen

$$2^1 \,.\, 3^3 = 54$$

eine Zahl sein, deren niedrigste Potenz, welche congruent 1 nach Modul 73 ist, jedenfalls grösser als 12 sein muss.

Die Division der successiven Potenzen von 54

$$54,\ 54^2,\ 54^3,\ 54^4,\ 54^5,\ 54^6,\ 54^7,\ 54^8,\ 54^9,\ 54^{10},\ 54^{11},\ 54^{12},$$
$$54^{13},\ 54^{14},\ 54^{15},\ 54^{16},\ 54^{17},\ 54^{18},\ 54^{19},\ 54^{20},\ 54^{21},\ 54^{22},\ 54^{23},$$
$$54^{24},\ 54^{25},\ 54^{26},\ 54^{27},\ 54^{28},\ 54^{29},\ 54^{30},\ 54^{31},\ 54^{32},\ 54^{33},\ 54^{34},$$
$$54^{35},\ 54^{36}$$

ergiebt die Reste

54, 69, 3, 16, 61, 9, 48, 37, 27, 71, 38, 8,
67, 41, 24, 55, 50, 72, 19, 4, 70, 57, 12, 64,
25, 36, 46, 2, 35, 65, 6, 32, 49, 18, 23, 1,

woraus wir ersehen, dass 36 die kleinste Zahl ist, welche der Congruenz

$$54^x \equiv 1 \pmod{73}$$

Genüge leistet.

Bei der Fortsetzung des Probierens müssen wir jetzt

eine Zahl nehmen, welche sich nicht unter den bereits gefundenen Resten befindet. Die kleinste unter den noch übrig bleibenden Zahlen ist 5 und indem wir die Zahl 5 zu allen successiven Potenzen, bis zur 72ten erheben und keine Zahl finden, welche nach Modul 73 congruent 1 wäre, überzeugen wir uns, dass die kleinste Zahl, welche der Congruenz

$$5^x \equiv 1 \pmod{73}$$

genügt, 72 ist. Dadurch ergiebt sich 5 als primitive Wurzel von 73.

Auf diese Weise finden wir *eine* der primitiven Wurzeln einer beliebigen Primzahl. Ist aber *eine* primitive Wurzel einer Zahl p gefunden, so kann man leicht auch alle übrigen aufstellen.

Es mag, in der That, a die gefundene primitive Wurzel von p sein, während $\alpha, \beta, \gamma, \ldots$ von einander verschiedene, in $p-1$ enthaltene Primzahlfactoren sein mögen. Ist dann A eine primitive Wurzel von p, so darf, nach Lehrsatz 48, keine der Congruenzen

$$x^\alpha \equiv A; \quad x^\beta \equiv A; \quad x^\gamma \equiv A; \quad \ldots; \pmod{p}$$

eine Lösung besitzen. Aus diesen Congruenzen folgt aber:

$$\alpha \,\text{Ind.}\, x \equiv \text{Ind.}\, A; \quad \beta \,\text{Ind.}\, x \equiv \text{Ind.}\, A; \quad \gamma \,\text{Ind.}\, x \equiv \text{Ind.}\, A; \ldots; \pmod{p-1}$$

und weil $\alpha, \beta, \gamma, \ldots$ in $p-1$ enthaltene Primzahlfactoren sind, so ist die Unmöglichkeit der letzten Congruenzen in der Untheilbarkeit von Ind. A durch $\alpha, \beta, \gamma, \ldots$ enthalten. Mit anderen Worten, die Unmöglichkeit dieser Congruenzen, ist dadurch bedingt, dass Ind. A zu $p-1$ relativ prim ist. Nehmen wir nun als Basis des Index die von uns bereits gefundene primitive Wurzel a, so ist

$$A \equiv a^{\text{Ind.}\, A} \pmod{p}.$$

Daraus folgt, dass jede primitive Wurzel von p, nach Modul p congruent ist unserer primitiven Wurzel a, erhoben zu einer Potenz, deren Exponent relativ prim zu $p-1$ ist.

Beispiel. Es ist leicht alle primitiven Wurzeln von 17 herzuleiten, sobald die eine primitive Wurzel 3 gefunden ist.

Man erhält nämlich alle primitiven Wurzeln aus den Congruenzen

$$x \equiv 3;\ x \equiv 3^3;\ x \equiv 3^7;\ x \equiv 3^9;\ x \equiv 3^{11};\ x \equiv 3^{13};\ x \equiv 3^{15} \pmod{17},$$

woraus erhellt, dass

$$3,\ 10,\ 11,\ 14,\ 7,\ 12,\ 6$$

sämmtliche primitive Wurzeln von 17 sind.

---

§ 41. Ueber die Anzahl der primitiven Wurzeln.

Auf Grund der ebenauseinandergesetzten Methode zur Auffindung der primitiven Wurzeln ergiebt sich die

Folgerung. In der Reihe der Zahlen

$$1,\ 2,\ \ldots,\ p-1$$

befinden sich genau so viele primitive Wurzeln von p, als es Zahlen giebt, welche kleiner als $p-1$ und zu $p-1$ relativ prim sind.

Man kann diesen Satz auch unmittelbar aus den in § 33 gezeigten Eigenschaften der primitiven Wurzeln herleiten.

Um nämlich alle unter den Zahlen

$$1,\ 2,\ 3,\ \ldots,\ p-1$$

enthaltenen primitiven Wurzeln von p zu erhalten, braucht man nur alle diejenigen Zahlen dieser Reihe fortzulassen, welche keine primitiven Wurzeln sein können. Nach § 38 heisst dieses aber nicht anders, als aus dieser Reihe alle Zahlen fortlassen, welche die Congruenzen

$$x^{\frac{p-1}{\alpha}} \equiv 1;\ x^{\frac{p-1}{\beta}} \equiv 1;\ x^{\frac{p-1}{\gamma}} \equiv 1;\ \ldots\ldots;\ \pmod{p},$$

befriedigen, wenn $\alpha, \beta, \gamma, \ldots\ldots$ in $p-1$ enthaltene Primzahlfactoren sind.

Darauf gegründet, können wir leicht abzählen, wie viele primitive Wurzeln von p sich unter den Zahlen

$$1, 2, 3, \ldots, p-1$$

befinden.

Wir beginnen mit dem einfachsten Falle, wenn $p-1$ nur durch die eine Primzahl α theilbar ist; es sei also $p-1 = \alpha^m$. In diesem Falle werden alle Zahlen der Reihe

$$1, 2, 3, \ldots, p-1,$$

welche die Congruenz

$$x^{\frac{p-1}{\alpha}} \equiv 1 \text{ (mod. } p)$$

nicht befriedigen, primitive Wurzeln von p sein. Nach Lehrsatz 35 befinden sich aber $\frac{p-1}{\alpha}$ Zahlen in der genannten Reihe, welche die letzte Congruenz befriedigen; folglich werden hier alle $p-1-\frac{p-1}{\alpha} = (p-1)\left(1-\frac{1}{\alpha}\right)$ übrigen Zahlen primitive Wurzeln sein. Nach Lehrsatz 12 giebt aber $(p-1)\left(1-\frac{1}{\alpha}\right)$ genau an, wie viele Zahlen kleiner als $p-1$ und relativ prim zu $p-1$ sind, wenn $p-1 = \alpha^m$ ist.

Wir wenden uns jetzt zu dem Falle, wenn $p-1$ durch zwei Primzahlen, α, β theilbar ist, also $p-1 = \alpha^m \beta^n$.

In diesem Falle findet man alle unter den Zahlen

$$1, 2, 3, \ldots, p-1$$

enthaltenen primitiven Wurzeln, wenn man in dieser Reihe die Zahlen, welche den Congruenzen

$$x^{\frac{p-1}{\alpha}} \equiv 1; \quad x^{\frac{p-1}{\beta}} \equiv 1 \text{ (mod. } p)$$

genügen, weglässt. Nach Lehrsatz 35 genügen der ersteren Congruenz $\frac{p-1}{\alpha}$ Zahlen, welche kleiner als p sind, während der letzteren $\frac{p-1}{\beta}$ solcher Zahlen genügen. Dann werden aber unter den Zahlen

$$1, 2, 3, \ldots, p-1$$

$\frac{p-1}{\alpha\beta}$ Zahlen sein, welche beide Congruenzen

$$x^{\frac{p-1}{\alpha}} \equiv 1; \quad x^{\frac{p-1}{\beta}} \equiv 1 \pmod{p}$$

gleichzeitig befriedigen, indem sie der Congruenz

$$x^{\frac{p-1}{\alpha\beta}} \equiv 1 \pmod{p}$$

Genüge leisten. Voneinander verschiedene Zahlen, welche den Congruenzen

$$x^{\frac{p-1}{\alpha}} \equiv 1; \quad x^{\frac{p-1}{\beta}} \equiv 1 \pmod{p}$$

genügen, giebt es somit

$$\frac{p-1}{\alpha} + \frac{p-1}{\beta} - \frac{p-1}{\alpha\beta}.$$

Schliesst man diese aus der Reihe

$$1, 2, 3, \ldots, p-1$$

aus, so sind alle

$$p-1 - \frac{p-1}{\alpha} - \frac{p-1}{\beta} + \frac{p-1}{\alpha\beta} = (p-1)\left(1-\frac{1}{\alpha}\right)\left(1-\frac{1}{\beta}\right)$$

übrigbleibende Zahlen primitive Wurzeln. Nach Lehrsatz 12 wissen wir aber, dass

$$(p-1)\left(1-\frac{1}{\alpha}\right)\left(1-\frac{1}{\beta}\right)$$

angiebt, wie viele Zahlen kleiner als $p-1$ und zu $p-1$ relativ prim sind, wenn $p-1 = \alpha^m \beta^n$ ist.

In ähnlicher Weise

$$\text{für } p-1 = \alpha^m \beta^n \gamma^r, \text{ dann für } p-1 = \alpha^m \beta^n \gamma^r \delta^\varepsilon$$

und so weiter fortfahrend, beweisen wir, dass allgemein unter den Zahlen

$$1, 2, 3, \ldots, p-1$$

immer genau so viele primitive Wurzeln von p vorhanden sind als es Zahlen giebt, welche kleiner als $p-1$ und zu $p-1$ relativ prim sind, wie in unserem Satze ausgesprochen war.



Man kann nun beliebig irgend eine der primitiven Wurzeln von p als Basis wählen, um den Index in Bezug auf Modul p zu bestimmen. Am bequemsten ist es immer solche zu wählen, welche am leichtesten zu Potenzen zu erheben sind, um so am leichtesten durch sie den Index zu bestimmen.

Uebrigens ist es aber leicht, wenn der Index in Bezug auf *eine* Basis gegeben ist, daraus den Index in Bezug auf eine *andere* Basis herzuleiten.

Es sei nämlich a diejenige Basis, nach welcher die Tabelle zusammengestellt ist und b mag diejenige Basis sein, in Bezug auf welche wir den Index irgend einer Zahl A zu berechnen wünschen. Bezeichnet man den Index von A in Bezug auf die Basis b mit x, so erhält man zur Bestimmung von x die Congruenz

$$A \equiv b^x \pmod{p}.$$

Aus dieser Congruenz schliessen wir, dass der Index von A dem b^x gleich ist, in Bezug auf welche Basis a man den Index auch nehmen mag. Man hat also in Bezug auf die den Tabellen zu Grunde gelegte Basis a

$$\text{Ind.}\, A = \text{Ind.}\, b^x.$$

Nach der Eigenschaft des Index überhaupt, erhält man aber

$$\text{Ind.}\, b^x \equiv x\, \text{Ind.}\, b \pmod{p-1},$$

folglich

$$x\, \text{Ind.}\, b \equiv \text{Ind.}\, A \pmod{p-1}.$$

Die Lösung dieser Congruenz liefert dann x.

Diese Congruenz wird immer eine Lösung haben, weil der Index einer primitiven Wurzel, wie wir gesehen haben, immer zu $p-1$ relativ prim ist. Indem wir diese Congruenz lösen, finden wir leicht eine positive Zahl, welche kleiner als $p-1$ ist und die Congruenz befriedigt. Diese Zahl ist dann der gesuchte Index x der Zahl A in Bezug auf die Basis b.

Beispiel. Wir wollen den Index der Zahl 25 in Bezug auf die Basis 2 und den Modul 29 aufsuchen, wenn



wir den Index aller Zahlen in Bezug auf denselben Modul und die Basis 10, wie dieses in den Tabellen angegeben ist, bereits kennen.

Bezeichnen wir den gesuchten Index mit x, so erhalten wir für seine Bestimmung

$$x \,.\, \text{Ind.}\,2 \equiv \text{Ind.}\,25 \pmod{28}.$$

Es ist aber

$$\text{Ind.}\,2 = 11; \quad \text{Ind.}\,25 = 8,$$

folglich wird x aus der Congruenz

$$11\,x \equiv 8 \pmod{28}$$

bestimmt.

Indem wir diese Congruenz auflösen, finden wir

$$x \equiv 16 \pmod{28},$$

und somit ist 16 der Index von 25 in Bezug auf die Basis 2.

Kapitel VII.

Ueber Congruenzen zweiten Grades mit zwei Unbekannten.

§ 42. Ueber die Congruenz
$$x^2 + Ay^2 + B \equiv 0 \pmod{p}.$$

Bis jetzt haben wir uns ausschliesslich mit Congruenzen beschäftigt, welche nur *eine* Unbekannte enthalten; nunmehr wollen wir zur Betrachtung von Congruenzen mit *zwei* Unbekannten übergehen. Die bemerkenswerthesten unter ihnen, welche zugleich bis jetzt am meisten Anwendungen zulassen, sind die Congruenzen zweiten Grades von der Gestalt

$$x^2 + Ay^2 + B \equiv 0 \pmod{p};$$

mit diesen wollen wir uns nun eingehend beschäftigen.

Wir beweisen zunächst über Congruenzen dieser Gestalt folgenden

49. *Lehrsatz.* *Ist p eine Primzahl und kein Theiler von A, so kann die Congruenz*

$$x^2 + Ay^2 + B \equiv 0 \pmod{p}$$

immer [durch ganze positive Zahlen] *befriedigt werden.*

Beweis. Die Behauptung dieses Lehrsatzes ist zunächst offenbar richtig für $p = 2$; weil dann die Congruenz

$$x^2 + Ay^2 + B \equiv 0 \pmod{p}$$

durch $y = 0$; $x = B$ befriedigt wird. Ebenso einleuchtend ist die Richtigkeit der Behauptung in dem Falle, wenn für irgend einen Werth von y die Summe

$$Ay^2 + B$$

ein Vielfaches von p wird; weil ein solcher Werth von y zusammen mit $x = 0$ die Congruenz

$$x^2 + Ay^2 + B \equiv 0 \pmod{p}$$

befriedigt.

Wir wollen nun die Möglichkeit, diese Congruenz zu befriedigen, für den Fall, wenn

$$p > 2 \quad \text{und} \quad Ay^2 + B$$

durch p untheilbar ist, beweisen.

In diesem Falle wird sich unter allen Werthen von $-Ay^2-B$, welche den p Werthen von y, von $y = 0$ bis $y = p-1$, entsprechen, eine Zahl sicher finden, welche nach Modul p congruent x^2 ist. Denn die Unmöglichkeit der Congruenz

$$x^2 \equiv -Ay^2-B \pmod{p},$$

wenn p eine Primzahl, grösser als 2, und $-Ay^2-B$ durch p untheilbar ist, würde nach dem, was wir in Kapitel IV gesehen haben, auf die Congruenz

$$(-Ay^2-B)^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}$$

führen, welche, nach dem binomischen Satze entwickelt, die Form

$$\pm A^{\frac{p-1}{2}} y^{p-1} \pm \frac{p-1}{2} A^{\frac{p-3}{2}} By^{p-3} \pm \ldots \pm B^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}$$

annimmt.

Dieser Congruenz können nicht alle p Zahlen

$$0, 1, 2, \ldots, p-1$$

zugleich Genüge leisten, weil die Congruenz vom Grade $p-1$ ist, während der Coefficient von y^{p-1}, nämlich $A^{\frac{p-1}{2}}$, als Potenz einer Zahl A, welche relativ prim zu p vorausgesetzt war, nicht durch p theilbar sein kann.

Somit wird mindestens *eine* den Zahlen

$$0, 1, 2, \ldots, p-1$$

die letztgenannte Congruenz nicht befriedigen. Diese Zahl verwandelt aber $-Ay^2-B$ in einen quadratischen Rest von p; für einen solchen Werth von $-Ay^2-B$ kann man, wie wir wissen, immer eine Zahl x finden, welche die Congruenz

$$x^2 \equiv -Ay^2-B \pmod{p}$$

befriedigt, wodurch der Lehrsatz bewiesen ist.

Wir erhalten, als speciellen Fall des bewiesenen Lehrsatzes, den

Zusatz. Die Congruenz

$$x^2+y^2+1 \equiv 0 \pmod{p}$$

besitzt immer eine Lösung.

---

§ 43. Ueber die Theiler der quadratischen Form $x^2 \pm Ay^2$.

Wir wollen uns ein wenig bei der Untersuchung der Congruenz

$$x^2+Ay^2+C \equiv 0 \pmod{M}$$

aufhalten, in dem speciellen Falle, wenn

$$C = 0$$

ist. Der Gegenstand unserer Untersuchung soll in der Beantwortung der Frage bestehen,

welche Eigenschaften muss die Zahl M besitzen damit die Congruenz

$$x^2+Ay^2 \equiv 0 \pmod{M}$$

durch irgend welche Zahlen x, y, welche relativ prim zu einander sind, befriedigt werde?

Die Möglichkeit dieser Congruenz in dem angegebenen Sinne zeigt, dass M ein Theiler der durch die Form x^2+Ay^2 dargestellten Zahl sein kann, während x, y relativ prim zu einander sind. Im entgegengesetzten Falle

sind die durch $x^2 + Ay^2$ dargestellten Zahlen durch M nicht theilbar.

Im ersteren Falle werden wir sagen: M ist Theiler der quadratischen Form $x^2 + Ay^2$; im anderen Falle: M ist Nichttheiler der quadratischen Form.

Wir werden dann Mittel angeben, durch welche man alle Theiler und Nichttheiler einer gegebenen Form finden kann. Diese Zahlen werden wir entweder in der Form $mz + \alpha$ darstellen, wobei z eine beliebige Zahl sein soll, oder in der Form

$$au^2 + 2buv + cv^2,$$

wobei u, v beliebige ganze Zahlen, die zu einander relativ prim sind, bedeuten.

Erstere machen Untersuchungen aus, welche unter dem Namen: *Theorie der linearen Theiler quadratischer Formen;* die zweiten: *Theorie der quadratischen Theiler quadratischer Formen* bekannt sind.

Wir beginnen mit der Theorie der linearen Theiler und beweisen zunächst einen Lehrsatz, welcher für die ganze Theorie von fundamentaler Bedeutung ist.

50. *Lehrsatz. Befriedigen irgend welche Zahlen x, y, die zu einander relativ prim sind, die Congruenz*

$$x^2 + Ay^2 \equiv 0 \pmod{M},$$

so besitzt die Congruenz

$$u^2 + A \equiv 0 \pmod{M}$$

jedenfalls eine Lösung.

Beweis. Wenn, in der That, x und y, ohne einen gemeinsamer Theiler zu haben, die Congruenz

$$x^2 + Ay^2 \equiv 0 \pmod{M}$$

befriedigen, so muss y relativ prim zu M sein; da im entgegengesetzten Falle, irgend eine Primzahl, welche zugleich M und y theilt, auch x theilen müsste und es hätten somit x und y einen gemeinsamen Theiler. Ist aber y relativ prim zu M, so kann man offenbar eine

Zahl u finden, welche die Congruenz

$$yu \equiv x \pmod{M}$$

befriedigt.

Erhebt man beide Seiten dieser letzteren zum Quadrat, so liefert die Congruenz

$$y^2 u^2 \equiv x^2 \pmod{M},$$

zusammen mit der gegebenen

$$x^2 + Ay^2 \equiv 0 \pmod{M},$$

die neue Congruenz

$$y^2 u^2 + Ay^2 \equiv 0 \pmod{M}.$$

Da nun y relativ prim zu M war, so darf man die letzte Congruenz durch y^2 dividiren und man erhält somit

$$u^2 + A \equiv 0 \pmod{M},$$

was zu beweisen war.

Die Möglichkeit, die Congruenz

$$x^2 + Ay^2 \equiv 0 \pmod{M}$$

durch x, y, welche relativ prim zu einander sind, zu befriedigen, bedingt somit die Möglichkeit die Congruenz

$$u^2 + A \equiv 0 \pmod{M}$$

zu befriedigen.

Kann man, umgekehrt, die letzte Congruenz befriedigen, so kann man offenbar die Congruenz

$$x^2 + Ay^2 \equiv 0 \pmod{p}$$

dadurch befriedigen, dass man

$$y = 1; \; x = u$$

setzt.

Auf Grund des bewiesenen Lehrsatzes kann man [in vielen Fällen] leicht erkennen, ob eine gegebene Zahl Theiler einer gegebenen Form ist, oder nicht.

Beispiele. 1) *Wir wollen untersuchen, ob man die Congruenz*

$$x^2 - 3y^2 \equiv 0 \pmod{5}$$

durch x, y, *welche relativ prim zu einander sind, befriedigen kann.* Mit anderen Worten, *ob 5 ein Theiler der Form* $x^2 - 3y^2$ *sein kann.*

Da wir nach der in Kapitel IV angegebenen Methode den Werth des Legender'schen Symbols $\left(\frac{3}{5}\right) = -1$ finden, so schliessen wir daraus, dass die Congruenz

$$u^2 - 3 \equiv 0 \pmod{5}$$

keine Lösung besitzt. Daraus folgt, auf Grund des oben bewiesenen Lehrsatzes, dass *es nicht möglich ist, die Congruenz*

$$x^2 - 3y^2 \equiv 0 \pmod{5}$$

durch x, y, *welche relativ prim zu einander sind, zu befriedigen;* mit anderen Worten, *dass es nicht möglich ist* $x^2 - 3y^2$ *in ein Vielfaches von 5 zu verwandeln.*

---

2) *Es sei gegeben*

$$x^2 + y^2 \equiv 0 \pmod{p},$$

wobei p *eine Primzahl von der Form* $4n + 3$ *ist.*

Da wir wissen, dass für eine Primzahl p von der Form $4n + 3$ immer

$$\left(\frac{-1}{p}\right) = -1$$

ist, so kann die Congruenz

$$u^2 + 1 \equiv 0 \pmod{p}$$

keine Lösung besitzen *und es ist somit nicht möglich* die Congruenz

$$x^2 + y^2 \equiv 0 \pmod{p}$$

durch x, y, welche relativ prim zu einander sind, zu befriedigen.

Daraus folgt, dass keine Primzahl von der Form $4n + 3$ Theiler einer Zahl sein kann, welche als Summe der Quadrate zweier Zahlen, die zu einander relativ prim sind, darstellbar ist.

So sind z. B. die Zahlen

$$5 = 2^2 + 1;\quad 10 = 3^2 + 1\ ;\quad 13 = 3^2 + 2^2,$$
$$17 = 4^2 + 1;\quad 25 = 4^2 + 3^2;\quad 26 = 5^2 + 1\ , \ldots .$$

durch die Zahlen

7, 11, 19, 23 von der Form $4n + 3$

nicht theilbar.

---

3) *Es sei die Congruenz*

$$x^2 + y^2 \equiv 0 \pmod{p}$$

gegeben, wenn p eine Primzahl von der Form $4n+1$ ist.

Da wir wissen, dass wenn p eine Primzahl von der Form $4n+1$ ist, immer

$$\left(\frac{-1}{p}\right) = +1$$

und dass somit die Congruenz

$$u^2 + 1 \equiv 0 \pmod{p}$$

möglich ist, so folgt daraus *die Möglichkeit, die Congruenz*

$$x^2 + y^2 \equiv 0 \pmod{p}$$

durch x, y, welche relativ prim zu einander sind, zu befriedigen, oder, was dasselbe ist: *die Theilbarkeit einer Summe zweier Quadrate durch $p = 4n+1$.*

Man kann auch allgemein auf Grund des oben bewiesenen Lehrsatzes leicht die Form einer Primzahl p erkennen, welche Theiler einer gegebenen quadratischen Form $x^2 + Ay^2$ sein kann.

Wir wollen uns nicht bei dem Falle $p = 2$ aufhalten, weil 2 immer Theiler von $x^2 + Ay^2$ ist, entweder für $x = 1$; $y = 1$, oder für $x = 0$; $y = 1$. Wir werden daher im Folgenden immer voraussetzen können, dass p eine von 2 verschiedene Primzahl ist.

Bevor wir aber dazu übergehen, wollen wir einige allgemeinere Lehrsätze beweisen.

51. *Lehrsatz.* *Ist A eine Primzahl von der Form $4n+3$ und M ein ungerader Theiler der quadratischen Form*

$$x^2 + Ay^2,$$

so ist

$$\left(\frac{M}{A}\right) = +1.$$

Beweis. Ist M Theiler der quadratischen Form

$$x^2 + Ay^2,$$

so kann die Congruenz

$$x^2 + Ay^2 \equiv 0 \pmod{M}$$

durch x, y, welche relativ prim zu einander sind, befriedigt werden, was nach Lehrsatz 50 die Möglichkeit der Congruenz

$$u^2 + A \equiv 0 \pmod{M}$$

bedingt.

Denkt man sich M als Product der Primzahlfactoren $\alpha, \beta, \gamma, \ldots.$ dargestellt, so kann man die Möglichkeit der Congruenz

$$u^2 + A \equiv 0 \pmod{M},$$

nach § 30 [Umkehrung], durch das System der Gleichungen

$$\left(\frac{-A}{\alpha}\right) = 1; \quad \left(\frac{-A}{\beta}\right) = 1; \quad \left(\frac{-A}{\gamma}\right) = 1; \ldots.$$

ausdrücken.

Es ist aber leicht aus diesen Gleichungen die Werthe der Symbole $\left(\frac{\alpha}{A}\right)$; $\left(\frac{\beta}{A}\right)$; $\left(\frac{\gamma}{A}\right)$; .... herzuleiten; und zwar wird

$$\left(\frac{\alpha}{A}\right) = 1; \quad \left(\frac{\beta}{A}\right) = 1; \quad \left(\frac{\gamma}{A}\right) = 1; \ldots.$$

So finden wir z. B. für das erste dieser Symbole nach den im IVten Kapitel bewiesenen Eigenschaften von $\left(\frac{p}{q}\right)$, dass

$$\left(\frac{\alpha}{A}\right) = \left(\frac{A}{\alpha}\right)(-1)^{\frac{\alpha-1}{2}\cdot\frac{A-1}{2}} = \left(\frac{-A}{\alpha}\right)(-1)^{\frac{\alpha-1}{2}+\frac{\alpha-1}{2}\cdot\frac{A-1}{2}},$$

also:

$$\left(\frac{\alpha}{A}\right) = \left(\frac{-A}{\alpha}\right)(-1)^{\frac{\alpha-1}{2}\cdot\frac{A+1}{2}}.$$

Da aber nach den obigen Gleichungen $\left(\frac{-A}{\alpha}\right) = 1$ ist und A nach der Voraussetzung die Gestalt $4n + 3$ hat, so erhalten wir aus der letzten Gleichung

$$\left(\frac{\alpha}{A}\right) = 1.$$

In ähnlicher Weise erhalten wir

$$\left(\frac{\beta}{A}\right) = 1; \quad \left(\frac{\gamma}{A}\right) = 1; \quad \ldots\ldots$$

Durch Multiplication dieser Symbole erhält man

$$\left(\frac{\alpha}{A}\right)\left(\frac{\beta}{A}\right)\left(\frac{\gamma}{A}\right)\ldots\ldots = \left(\frac{\alpha\beta\gamma\ldots}{A}\right) = 1$$

und, wenn man darin

$$M = \alpha\beta\gamma\ldots$$

setzt, ergiebt sich

$$\left(\frac{M}{A}\right) = 1;$$

[offenbar folgt aus

$$\left(\frac{\alpha}{A}\right) = 1; \quad \left(\frac{\beta}{A}\right) = 1; \quad \left(\frac{\gamma}{A}\right) = 1; \ldots$$

zugleich auch

$$\left(\frac{\alpha}{A}\right)^m\left(\frac{\beta}{A}\right)^n\left(\frac{\gamma}{A}\right)^r\ldots = \left(\frac{\alpha^m\beta^n\gamma^r\ldots}{A}\right) = 1,$$

also auch, wenn

$$M = \alpha^m\beta^n\gamma^r\ldots$$

gesetzt wird, $\left(\frac{M}{A}\right) = 1$]; was wir beweisen wollten.

52. *Lehrsatz.* *Ist A eine Primzahl von der Gestalt $4n+1$, während M ein ungerader Theiler von x^2+Ay^2 ist, so wird*

$$\left(\frac{M}{A}\right) = (-1)^{\frac{M-1}{2}},$$

d. h.

$$\left(\frac{M}{A}\right) = 1, \text{ wenn } M = 4m+1;$$

$$\left(\frac{M}{A}\right) = -1, \text{ wenn } M = 4m+3.$$

Beweis. Ist M Theiler von x^2+Ay^2, so besitzt die Congruenz

$$x^2 + Ay^2 \equiv 0 \pmod{M},$$

also auch die Congruenz

$$u^2 + A \equiv 0 \pmod{M}$$

eine Lösung. Dieses setzt aber, wie wir [§ 30, Umkehrung] gesehen haben, die Gleichungen

$$\left(\frac{-A}{\alpha}\right) = 1; \quad \left(\frac{-A}{\beta}\right) = 1; \quad \left(\frac{-A}{\gamma}\right) = 1; \ldots.$$

voraus, wobei $\alpha, \beta, \gamma, \ldots$ die in M auftretenden Primzahlfactoren bedeuten.

Auf Grund der Eigenschaften des Symbols $\left(\frac{M}{q}\right)$ leiten wir aus den letzten Gleichungen die Werthe der Symbole $\left(\frac{\alpha}{A}\right)$, $\left(\frac{\beta}{A}\right)$, $\left(\frac{\gamma}{A}\right)$, ... her.

So erhalten wir für den Werth des ersteren

$$\left(\frac{\alpha}{A}\right) = \left(\frac{A}{\alpha}\right)(-1)^{\frac{\alpha-1}{2}\cdot\frac{A-1}{2}} = \left(\frac{-A}{\alpha}\right)(-1)^{\frac{\alpha-1}{2}+\frac{\alpha-1}{2}\cdot\frac{A-1}{2}}$$

$$= \left(\frac{-A}{\alpha}\right)(-1)^{\frac{\alpha-1}{2}\cdot\frac{A+1}{2}},$$

also, genau wie im Lehrsatze 51, mit Berücksichtigung des

Werthes $\left(\frac{-A}{\alpha}\right) = 1$:

$$\left(\frac{\alpha}{A}\right) = (-1)^{\frac{\alpha-1}{2}\cdot\frac{A+1}{2}}.$$

Da aber diesmal, nach Voraussetzung, A die Gestalt $A = 4n + 1$ hat, so ist

$$(-1)^{\frac{\alpha-1}{2}\cdot\frac{A+1}{2}} = (-1)^{\frac{\alpha-1}{2}\cdot\frac{4n+2}{2}} = (-1)^{\frac{\alpha-1}{2}(2n+1)} = (-1)^{\frac{\alpha-1}{2}},$$

folglich ist:

$$\left(\frac{\alpha}{A}\right) = (-1)^{\frac{\alpha-1}{2}}.$$

In ähnlicher Weise erhalten wir

$$\left(\frac{\beta}{A}\right) = (-1)^{\frac{\beta-1}{2}}; \quad \left(\frac{\gamma}{A}\right) = (-1)^{\frac{\gamma-1}{2}}; \ldots.$$

Die Multiplication der Gleichungen für

$$\left(\frac{\alpha}{A}\right), \left(\frac{\beta}{A}\right), \left(\frac{\gamma}{A}\right), \ldots$$

ergiebt dann

$$\left(\frac{\alpha}{A}\right)\left(\frac{\beta}{A}\right)\left(\frac{\gamma}{A}\right)\ldots = (-1)^{\frac{\alpha-1}{2}+\frac{\beta-1}{2}+\frac{\gamma-1}{2}+\ldots},$$

woraus für $M = \alpha\,\beta\,\gamma \ldots.$ folgt:

$$\left(\frac{M}{A}\right) = (-1)^{\frac{\alpha-1}{2}+\frac{\beta-1}{2}+\frac{\gamma-1}{2}+\ldots}.$$

Man kann sich aber leicht überzeugen, dass die beiden Zahlen

$$\frac{M-1}{2} \quad \text{und} \quad \frac{\alpha-1}{2}+\frac{\beta-1}{2}+\frac{\gamma-1}{2}+\ldots$$

um eine gerade Zahl von einander differiren. Denn, es ist, wenn $M = \alpha\,\beta\,\gamma \ldots.$ gesetzt wird,

$$\frac{M-1}{2} = \frac{\alpha\,\beta\,\gamma \ldots. -1}{2},$$

was man auch so schreiben kann:

$$\frac{-1+\left(1+2\,\frac{\alpha-1}{2}\right)\left(1+2\,\frac{\beta-1}{2}\right)\left(1+2\,\frac{\gamma-1}{2}\right)\cdots\cdot}{2}.$$

Indem man in diesem Ausdrucke die Multiplication der Klammerinhalte ausführt und diejenigen Glieder des Resultats, welche den Factor 2 haben, vernachlässigt, erhält man

$$\frac{\alpha-1}{2}+\frac{\beta-1}{2}+\frac{\gamma-1}{2}+\cdots\cdot$$

übrig; so dass diese Zahl sich nur um eine gerade Zahl von $\frac{M-1}{2}$ unterscheidet. Es ist also

$$(-1)^{\frac{\alpha-1}{2}+\frac{\beta-1}{2}+\frac{\gamma-1}{2}+\cdots}=(-1)^{\frac{M-1}{2}}$$

und infolgedessen verwandelt sich der oben gefundene Werth von $\left(\frac{M}{A}\right)$ in

$$\left(\frac{M}{A}\right)=(-1)^{\frac{M-1}{2}}.$$

[Man kann leicht einsehen, dass sich in der ganzen Beweisführung nichts ändert, wenn zugelassen wird, dass beliebig viele unter den Primzahlen α, β, γ, ... einander gleich sein können. Dadurch ist dann auch die Gültigkeit des Satzes für eine Zahl M von der Gestalt $M=\alpha^m\beta^n\gamma^r\ldots$ erwiesen. Uebrigens complicirt sich auch die directe Beweisführung unter der Voraussetzung $M=\alpha^m\beta^n\gamma^r\ldots$ nur wenig.

Es ergiebt sich nämlich aus

$$\left(\frac{\alpha}{A}\right)=(-1)^{\frac{\alpha-1}{2}};\ \left(\frac{\beta}{A}\right)=(-1)^{\frac{\beta-1}{2}};\ \left(\frac{\gamma}{A}\right)=(-1)^{\frac{\gamma-1}{2}};\ldots$$

zunächst

$$\left(\frac{\alpha}{A}\right)^m\left(\frac{\beta}{A}\right)^n\left(\frac{\gamma}{A}\right)^r\cdots=\left(\frac{\alpha^m\beta^n\gamma^r\ldots}{A}\right)=(-1)^{m\frac{\alpha-1}{2}+n\frac{\beta-1}{2}+r\frac{\gamma-1}{2}+\cdots}$$

also, wenn $M=\alpha^m\beta^n\gamma^r\ldots$ gesetzt wird:

$$\left(\frac{M}{A}\right) = (-1)^{m\frac{\alpha-1}{2} + n\frac{\beta-1}{2} + r\frac{\gamma-1}{2} + \dots}.$$

Man kann aber leicht einsehen, dass die beiden Zahlen

$$\frac{M-1}{2} \text{ und } m\frac{\alpha-1}{2} + n\frac{\beta-1}{2} + r\frac{\gamma-1}{2} + \dots$$

immer nur um eine gerade Zahl von einander differiren. Denn mit Berücksichtigung der Identitäten

$$\alpha = 1 + 2\frac{\alpha-1}{2};\ \beta = 1 + 2\frac{\beta-1}{2};\ \gamma = 1 + 2\frac{\gamma-1}{2};\dots$$

geht die Gleichung

$$\frac{M-1}{2} = \frac{\alpha^m \beta^n \gamma^r \dots -1}{2}$$

in

$$\frac{M-1}{2} = \frac{-1+\left(1+2\frac{\alpha-1}{2}\right)^m + \left(1+2\frac{\beta-1}{2}\right)^n \left(1+2\frac{\gamma-1}{2}\right)^r \dots}{2}$$

über.

Die Entwickelung nach dem binomischen Satze ergiebt:

$$\left(1+2\frac{\alpha-1}{2}\right)^m = 1+2\,.\,m\frac{\alpha-1}{2} + 2^2\,.\,\frac{m(m-1)}{1\,.\,2}\left(\frac{\alpha-1}{2}\right)^2 + \\ + \dots + 2^{m-1}\,.\,m\left(\frac{\alpha-1}{2}\right)^{m-1} + 2^m\left(\frac{\alpha-1}{2}\right)^m.$$

Da nun $M = \alpha^m \beta^n \gamma^r \dots$ ungerade vorausgesetzt war, so müssen auch $\alpha, \beta, \gamma, \dots$ alle ungerade sein, folglich ist $\frac{\alpha-1}{2}$ eine ganze Zahl. Bekanntlich sind die Binomialcoëfficienten $m, \frac{m(m-1)}{1\,.\,2}; \frac{m(m-1)(m-2)}{1\,.\,2\,.\,3}$; immer ganze Zahlen, sobald m eine ganze Zahl ist. Vgl. Anm. zu § 30. Man kann somit

$$\left(1 + 2\frac{\alpha-1}{2}\right)^m = 1 + 2\,.\,m\frac{\alpha-1}{2} + 2^2\,.\,\sigma_1$$

setzen, wenn man mit σ_1 die Summe aller übrigen Glieder der Entwickelung bezeichnet, welche alle den Factor 2 zu höheren Potenzen enthalten.

Ebenso erhält man

$$\left(1+2\frac{\beta-1}{2}\right)^n = 1+2\,.\,n\frac{\beta-1}{2}+2^2\,.\,\sigma_2$$

$$\left(1+2\frac{\gamma-1}{2}\right)^r = 1+2\,.\,r\frac{\gamma-1}{2}+2^2\,.\,\sigma_3$$

$$\vdots$$

Muultiplicirt man diese Resultate mit einander, so ergiebt sich

$$\left(1+2\frac{\alpha-1}{2}\right)^m\left(1+2\frac{\beta-1}{2}\right)^n\left(1+2\frac{\gamma-1}{2}\right)^r\ldots$$

$$= 1+2\left[m\frac{\alpha-1}{2}+n\frac{\beta-1}{2}+r\frac{\gamma-1}{2}+\ldots\right]+2^2\,S,$$

wenn man mit S die Summe aller übrigen Glieder des ausgerechneten Productes bezeichnet.

Setzt man diesen Werth in

$$\frac{M-1}{2}=\frac{-1+\left(1+2\frac{\alpha-1}{2}\right)^m\left(1+2\frac{\beta-1}{2}\right)^n\left(1+2\frac{\gamma-1}{2}\right)^r\ldots}{2}$$

ein, so erhält man:

$$\frac{M-1}{2}=m\frac{\alpha-1}{2}+n\frac{\beta-1}{2}+r\frac{\gamma-1}{2}+\ldots+2\,.\,S,$$

was aussagt, dass die beiden Zahlen

$$\frac{M-1}{2} \quad\text{und}\quad m\frac{\alpha-1}{2}+n\frac{\beta-1}{2}+r\frac{\gamma-1}{2}+\ldots$$

sich nur um eine gerade Zahl von einander unterscheiden. Da nun immer $(-1)^k = (-1)^{k+2S}$ ist, so darf man, anstatt

$$\left(\frac{M}{A}\right)=(-1)^{m\frac{\alpha-1}{2}+n\frac{\beta-1}{2}+r\frac{\gamma-1}{2}+\ldots},$$

auch

$$\left(\frac{M}{A}\right)=(-1)^{\frac{M-1}{2}},$$

schreiben, was zu beweisen war].

53. *Lehrsatz.* *Ist A eine Primzahl von der Gestalt $4n+1$ und M ein ungerader Theiler der Form*

$$x^2 - Ay^2,$$

so ist

$$\left(\frac{M}{A}\right) = 1.$$

Beweis. Ist M ein Theiler von x^2-Ay^2, so besteht die Congruenz

$$x^2 - Ay^2 \equiv 0 \pmod{M}.$$

Nach Lehrsatz 50 folgt daraus auch die Existenz von

$$u^2 - A \equiv 0 \pmod{M},$$

woraus sich nach § 30 [Umkehrung] die Gleichungen

$$\left(\frac{A}{\alpha}\right) = 1; \quad \left(\frac{A}{\beta}\right) = 1; \quad \left(\frac{A}{\gamma}\right) = 1; \quad \ldots .$$

ergeben, wenn α, β, γ, . . . in P enthaltene Primzahlfactoren bedeuten. Berechnet man aus der ersten dieser Gleichungen den Werth von $\left(\frac{\alpha}{A}\right)$, so erhält man auf Grund des Reciprocitätsgesetzes

$$\left(\frac{\alpha}{A}\right) = \left(\frac{A}{\alpha}\right)(-1)^{\frac{\alpha-1}{2}\cdot\frac{A-1}{2}} = (-1)^{\frac{\alpha-1}{2}\cdot\frac{A-1}{2}},$$

was nach der Voraussetzung $A = 4n+1$, also $\frac{A-1}{2} = 2n$, in

$$\left(\frac{\alpha}{A}\right) = 1$$

übergeht. Ebenso ergiebt sich

$$\left(\frac{\beta}{A}\right) = 1; \quad \left(\frac{\gamma}{A}\right) = 1; \quad \ldots$$

Durch Multiplication erhält man $\left(\frac{\alpha\beta\gamma\ldots}{A}\right) = 1$; oder, $M = \alpha\beta\gamma\ldots$ gesetzt, $\left(\frac{M}{A}\right) = 1$.

[Es ergiebt sich aus

$$\left(\frac{\alpha}{A}\right) = 1; \ \left(\frac{\beta}{A}\right) = 1; \ \left(\frac{\gamma}{A}\right) = 1; \ \ldots$$

ebensogut auch

$$\left(\frac{\alpha^m \beta^n \gamma^r \ldots}{A}\right) = 1;$$

also auch, wenn $M = \alpha^m \beta^n \gamma^r \ldots$ eingesetzt wird,

$$\left(\frac{M}{A}\right) = 1].$$

Das ist es, was wir beweisen wollten.

54. *Lehrsatz.* *Ist A eine Primzahl von der Gestalt $4n+3$ und M ein ungerader Theiler der Form*

$$x^2 - Ay^2,$$

so ist

$$\left(\frac{M}{A}\right) = (-1)^{\frac{M-1}{2}};$$

d. h. es ist

$$\left(\frac{M}{A}\right) = \quad 1, \ \textit{wenn} \ M = 4m+1$$

und

$$\left(\frac{M}{A}\right) = -1, \ \textit{wenn} \ M = 4m+3$$

ist.

Beweis. Wiederum schliessen wir zunächst aus der Theilbarkeit von x^2-Ay^2 durch M, d. h. aus der Congruenz

$$x^2-Ay^2 \equiv 0 \pmod{M}$$

über die Existenz von

$$u^2-A \equiv 0 \pmod{M},$$

woraus zunächst, wie im Lehrsatz 53, folgt:

$$\left(\frac{A}{\alpha}\right) = 1; \ \left(\frac{A}{\beta}\right) = 1; \ \left(\frac{A}{\gamma}\right) = 1, \ \ldots,$$

wenn α, β, γ von einander verschiedene, in M enthaltene, ungerade Primzahlfactoren bedeuten.

Auch hier erhält man dann

$$\left(\frac{\alpha}{A}\right) = (-1)^{\frac{\alpha-1}{2}\cdot\frac{A-1}{2}},$$

da aber in diesem Falle A, nach der Voraussetzung

$$A = 4n + 3; \quad \text{also} \quad \frac{A-1}{2} = 2n + 1,$$

eine ungerade Zahl ist, so wird

$$(-1)^{\frac{\alpha-1}{2}\cdot\frac{A-1}{2}} = (-1)^{\frac{\alpha-1}{2}2n + \frac{\alpha-1}{2}} = (-1)^{\frac{\alpha-1}{2}},$$

folglich erhält man:

$$\left(\frac{\alpha}{A}\right) = (-1)^{\frac{\alpha-1}{2}}; \left(\frac{\beta}{A}\right) = (-1)^{\frac{\beta-1}{2}}; \left(\frac{\gamma}{A}\right) = (-1)^{\frac{\gamma-1}{2}}; \ldots$$

Die Multiplication ergiebt, wie oben bei dem Beweise von Lehrsatz 52:

$$\left(\frac{\alpha}{A}\right)\left(\frac{\beta}{A}\right)\left(\frac{\gamma}{A}\right) \ldots\ldots = (-1)^{\frac{\alpha-1}{2}+\frac{\beta-1}{2}+\frac{\gamma-1}{2}+\ldots},$$

und folglich für $M = \alpha\beta\gamma\ldots.$

$$\left(\frac{M}{A}\right) = \left(\frac{\alpha\beta\gamma\ldots.}{A}\right) = (-1)^{\frac{\alpha-1}{2}+\frac{\beta-1}{2}+\frac{\gamma-1}{2}+\ldots}.$$

Da wir aber oben bereits gefunden, dass

$$(-1)^{\frac{\alpha-1}{2}+\frac{\beta-1}{2}+\frac{\gamma-1}{2}+\ldots} = (-1)^{\frac{M-1}{2}},$$

so ergiebt sich:

$$\left(\frac{M}{A}\right) = (-1)^{\frac{M-1}{2}}.$$

[Auch hier erhält man wie oben aus

$$\left(\frac{\alpha}{A}\right) = (-1)^{\frac{\alpha-1}{2}}; \quad \left(\frac{\beta}{A}\right) = (-1)^{\frac{\beta-1}{2}}; \quad \left(\frac{\gamma}{A}\right) = (-1)^{\frac{\gamma-1}{2}}$$

zunächst:

$$\left(\frac{\alpha}{A}\right)^m \left(\frac{\beta}{A}\right)^n \left(\frac{\gamma}{A}\right)^r \cdots = \left(\frac{\alpha^m \beta^n \gamma^r \cdots}{A}\right) = (-1)^{m\frac{\alpha-1}{2} + n\frac{\beta-1}{2} + r\frac{\gamma-1}{2} \cdots}$$

und weil, wie wir oben gesehen, wenn $M = \alpha^m \beta^n \gamma^r \ldots$ gesetzt wird,

$$(-1)^{m\frac{\alpha-1}{2} + n\frac{\beta-1}{2} + r\frac{\gamma-1}{2} + \cdots} = (-1)^{\frac{M-1}{2}}.$$

ist, so erhält man auch für $M = \alpha^m \beta^n \gamma^r \ldots$ die Gleichung

$$\left(\frac{M}{A}\right) = (-1)^{\frac{M-1}{2}}].$$

---

§ 44. Ueber die Bestimmung der Theiler einer Form $x^2 \pm Ay^2$, wenn A eine Primzahl ist.

Auf Grund der eben bewiesenen Lehrsätze kann man leicht alle linearen Theiler einer Form von der Gestalt

$$x^2 \pm Ay^2,$$

wenn A eine Primzahl ist, vollständig bestimmen.

Wir haben gesehen, dass die ungeraden Theiler solcher Formen

entweder durch die Gleichung $\left(\frac{M}{A}\right) = 1$,

oder durch die Gleichung $\left(\frac{M}{A}\right) = -1$

bestimmt werden, jenachdem 1) die Form $x^2 \pm Ay^2$ mit dem Vorzeichen $+$, oder mit dem Vorzeichen $-$ gegeben ist, jenachdem 2) A die Gestalt $4n+3$, oder $4n+1$ hat und in gewissen Fällen (S. Lehrss. 52 u. 54) jenachdem 3) M von der Gestalt $4m+1$, oder $4m+3$ ist.

Wir haben aber in § 28 eine Methode kennen gelernt, mittels welcher man leicht alle Zahlen finden kann, welche die Gleichung

$$\left(\frac{M}{A}\right) = 1$$

und ebenso alle, welche die Gleichung

$$\left(\frac{M}{A}\right) = -1$$

befriedigen. Es sind nämlich, wie wir dort gesehen haben, alle Lösungen der ersten Gleichung durch die Formeln

$$M = a_1 + nA; \quad M = a_2 + nA; \; \ldots.; \quad M = a_{\frac{A-1}{2}} + nA$$

dargestellt, wobei n eine willkürliche Zahl ist, während

$$a_1, \; a_2, \; \ldots., \; a_{\frac{A-1}{2}}$$

beziehungsweise diejenigen Reste bedeuten, welche nach der Division der Zahlen

$$1^2, \; 2^2, \; \ldots., \; \left(\frac{A-1}{2}\right)^2$$

durch A verbleiben. Die Lösungen der zweiten Gleichung

$$\left(\frac{M}{A}\right) = -1$$

sind durch die Formeln

$$M = b_1 + nA; \quad M = b_2 + nA; \; \ldots.; \quad M = b_{\frac{A-1}{2}} + nA$$

dargestellt, wobei mit

$$b_1, \; b_2, \; \ldots., \; b_{\frac{A-1}{2}}$$

diejenigen Zahlen aus der Reihe $1, 2, 3, \ldots, A-1$ bezeichnet werden, welche von den obigen Zahlen

$$a_1, \; a_2, \; \ldots., \; a_{\frac{A-1}{2}}$$

verschieden sind.

Wir wollen nun jetzt zusehen, wie jede dieser Formeln dazu dienen kann, Zahlen von der Gestalt $4m+1$, oder $4m+3$ zu bestimmen.

Damit eine Zahl M, welche durch die Gleichung

$$M = a + nA$$

definirt ist, die Gestalt $4m+1$ haben soll, muss n so be-

schaffen sein, dass die Summe $a + nA$ auf die Gestalt $4m + 1$ gebracht werden könnte; mit andern Worten, n muss die Congruenz

$$a + nA \equiv 1 \pmod{4}, \quad \text{oder} \quad nA \equiv 1 - a \pmod{4}$$

befriedigen.

Diese Congruenz wird immer *eine* Lösung besitzen, solange A eine ungerade Zahl ist. Indem wir diese Lösung nach der im § 15 gezeigten Methode aufsuchen, finden wir

$$n \equiv (1 - a) A^{4\frac{2-1}{2} - 1} \pmod{4},$$

oder, einfacher geschrieben:

$$n \equiv A(1 - a) \pmod{4}.$$

Dieser Congruenz wird immer eine der 4 Zahlen

$$0, \quad 1, \quad 2, \quad 3$$

genügen; bezeichnen wir jene Zahl mit r, so erhalten wir die Congruenz

$$r \equiv A(1 - a) \pmod{4},$$

infolgederen unsere obige Congruenz für n in

$$n \equiv r \pmod{4}$$

übergehen wird, woraus sich also für n die Gestalt:

$$n = 4z + r$$

ergiebt. Tragen wir diesen Werth von n in unser

$$M = nA + a$$

ein, so erhalten wir

$$M = 4Az + Ar + a$$

als Definition der Zahlen von der Gestalt $4m + 1$, welche die Gleichung $M = nA + a$ zu befriedigen haben.

In ganz ähnlicher Weise leiten wir für die Zahlen von der Gestalt $4m + 3$ die Formel

$$M = 4Az + Ar' + a,$$

her, wobei r' die kleinste Zahl bedeutet, welche $A(3 - a)$ nach Modul 4 congruent ist.

Auf diese Weise erhalten wir aus der Gleichung

$$M = nA + a,$$

welche eine der Lösungen von

$$\left(\frac{M}{A}\right) = 1$$

definirt, zwei Formeln

$$M = 4Az + Ar + a,$$
$$M = 4Az + Ar' + a,$$

von denen die erstere lauter Zahlen von der Gestalt $4m + 1$, während die letztere lauter Zahlen von der Gestalt $4m + 3$ liefert.

Es ist übrigens auch nicht schwer aus der Gleichung

$$M = nA + a$$

eine andere herzuleiten, welche zugleich die Zahlen von der Gestalt $4m + 1$ und $4m + 3$, also alle ungeraden Zahlen liefern wird. Zu diesem Zwecke müssen wir die Gestalt für die Zahl n aufsuchen, welche die Summe $nA + a$ in $2m + 1$ verwandelt; oder, mit andern Worten, wir müssen die Lösung der Congruenz

$$nA + a \equiv 1 \pmod{2}, \text{ also } nA \equiv (1 - a) \pmod{2}$$

aufsuchen.

Ist a eine ungerade Zahl, so genügt dieser Congruenz $n = 0$, folglich ist in diesem Falle die Lösung durch

$$n \equiv 0 \pmod{2}$$

dargestellt, woraus also

$$n = 2z$$

folgt.

Ist dagegen a gerade, so genügt $n = 1$ der obigen Congruenz (da A eine ungerade Zahl ist), folglich ist die Lösung durch

$$n = 2z + 1$$

dargestellt.

Trägt man diese Werthe in

$$M = nA + a$$

ein, so findet man für die Bestimmung der ungeraden Zahlen

$$M = 2Az + a, \quad \text{oder} \quad M = 2Az + A + a,$$

jenachdem a ungerade oder gerade ist.

Verfährt man ebenso mit jeder der Formeln

$$M = a_k + nA;$$
$$M = b_k + nA,$$

welche je eine Lösung der Gleichungen

$$\left(\frac{M}{A}\right) = 1; \quad \left(\frac{M}{A}\right) = -1$$

darstellen, so findet man *alle ungerade* Zahlen, welche der Bedingung

$$\left(\frac{M}{A}\right) = 1, \quad \text{oder} \quad \left(\frac{M}{A}\right) = -1$$

genügen, durch Formeln von der Gestalt

$$2Az + a$$

ausgedrückt; während alle Zahlen von der Gestalt $4m + 1$, oder alle von der Gestalt $4m + 3$ durch Formeln, wie

$$4Az + a$$

dargestellt werden.

Das sind die Formeln durch welche auf Grund der oben bewiesenen Lehrsätze, alle ungeraden Theiler der quadratischen Form $x^2 + Ay^2$ bestimmt werden.

Wir wollen die obige Auseinandersetzung durch Beispiele erläutern.

Beispiele. 1) Es werde die Gestalt aller ungeraden Theiler der quadratischen Form $x^2 + 19y^2$ gesucht.

Indem wir bemerken, dass 19 eine Primzahl und zwar von der Gestalt $4n + 3$ ist, so schliessen wir aus Lehrsatz 51, dass für die ungeraden Theiler M der gegebenen Form die Gleichung

$$\left(\frac{M}{19}\right) = 1$$

bestehen muss.

Um die Zahlen zu finden, welche dieser Gleichung genügen, dividiren wir

$$1^2,\ 2^2,\ 3^2,\ 4^2,\ 5^2,\ 6^2,\ 7^2,\ 8^2,\ 9^2$$

durch 19 und erhalten die Reste

$$1,\ 4,\ 9,\ 16,\ 6,\ 17,\ 11,\ 7,\ 5.$$

Daraus schliessen wir, dass die Zahlen M, welche der Gleichung

$$\left(\frac{M}{19}\right) = 1$$

genügen, durch irgend eine der Formeln

$$19n+1,\ 19n+4,\ 19n+9,\ 19n+16,\ 19n+6,$$
$$19n+17,\ 19n+11,\ 19n+7,\ 19n+5$$

dargestellt werden. Damit aber diese Formeln lauter ungerade Zahlen liefern sollen, müssen wir, nach der obigen Auseinandersetzung

die Formel $19n+1$ durch $2\,.\,19z+1$,
die Formel $19n+4$ durch $2\,.\,19z+19+4$,

u. s. w. ersetzen.

Auf diese Weise erhalten wir für die ungeraden Theiler der quadratischen Form

$$x^2+19y^2$$

die Formeln

$$2.19z+1;\ 2.19z+19+4;\ 2.19z+9;\ 2.19z+19+16;$$
$$2.19z+19+6;\ 2.19z+17;\ 2.19z+11;\ 2.19z+7;$$
$$2\,.\,19z+5,$$

welche, reducirt und geordnet, sich in folgende verwandeln:

$$38z+1,\ 38z+5,\ 38z+7,\ 38z+9,\ 38z+11,\ 38z+17,$$
$$38z+23,\ 38z+25,\ 38z+35.$$

Somit haben wir die nothwendige Gestalt aller ungeraden Zahlen gefunden, welche Theiler einer Summe x^2+19y^2 sein könnten, wenn x und y relativ prim zu einander sind.

Man kann die so gefundene nothwendige Gestalt dazu benutzen, um die Theiler irgend einer gegebenen Zahl zu finden, welche durch die Form

$$x^2 + 19y^2$$

darstellbar ist. So, z. B. mag die Zahl 2021 gegeben sein. Da dieselbe in der Form

$$11^2 + 19 \cdot 10^2$$

dargestellt werden kann, so müssen die Theiler derselben, wenn solche existiren, durch eine der Formeln

$$38z + 1,\ 38z + 5,\ 38z + 7,\ 38z + 9,\ 38z + 11,\ 38z + 17,$$
$$38z + 23,\ 38z + 25,\ 38z + 35$$

dargestellt werden können.

Wenn aber 2021 überhaupt Theiler besitzt, so muss jedenfalls einer derselben kleiner als

$$\sqrt{2021}, \text{ also kleiner als } 45$$

sein; diesen Theiler wollen wir eben aufsuchen.

Die erste Formel $38z + 1$ liefert einen solchen nicht; da dieselbe für $z = 0$ die Zahl 1 und für $z = 1$ die Zahl 39 liefert, welche kein Theiler von 2021 sein kann, weil letztere durch 3 nicht theilbar ist, während 39 den Factor 3 enthält. Für $z = 2$ und $z > 2$ ergiebt aber die Formel $38z + 1$ Zahlen, welche 45 übertreffen.

Wir wenden uns zur zweiten Formel $38z + 5$. Für $z = 0$ nimmt dieselbe den Werth 5 an, eine Zahl, welche offenbar kein Theiler von 2021 sein kann. Für $z = 1$ ergiebt die Formel die Zahl 43 und indem wir versuchen 2021 durch 43 zu dividiren, finden wir, dass 43 wirklich ein Theiler dieser Zahl ist. [Der zugehörige zweite Factor ist 47, derselbe wird aus der Formel $38z + 9$ für $z = 1$ erhalten. Alle übrigen Formeln liefern, wie leicht zu sehen, gar keinen Theiler.]

---

2) Als Beispiel für die Bestimmung der Theiler einer quadratischen Form von der Gestalt

$$x^2 - Ay^2,$$

wollen wir die Theiler der Form $x^2 - 7y^2$ aufsuchen.

Da die Zahl 7 von der Gestalt $4n + 3$ ist, so finden wir nach Lehrsatz 54, dass diejenigen Theiler der Form $x^2 - 7y^2$, welche die Gestalt $4m + 1$ haben, die Gleichung

$$\left(\frac{M}{7}\right) = 1,$$

während diejenigen Theiler, welche die Gestalt $4m + 3$ haben, die Gleichung

$$\left(\frac{M}{7}\right) = -1$$

befriedigen müssen.

Wir wollen zuerst diejenigen Zahlen von der Gestalt $4m + 1$, welche die Gleichung

$$\left(\frac{M}{7}\right) = 1$$

und diejenigen Zahlen von der Gestalt $4m + 3$, welche die Gleichung

$$\left(\frac{M}{7}\right) = -1$$

befriedigen, aufsuchen.

Um zunächst überhaupt die Zahlen zu finden, welche die Gleichung

$$\left(\frac{M}{7}\right) = 1$$

befriedigen, dividiren wir

$$1^2, \quad 2^2, \quad 3^2,$$

durch 7 und erhalten die Reste

$$1, \quad 4, \quad 2.$$

Folglich sind alle durch $\left(\frac{M}{7}\right) = 1$ definirten Zahlen durch

$$7n + 1, \quad 7n + 4, \quad 7n + 2$$

dargestellt.

Aus diesen Zahlen wollen wir nun solche herleiten, welche die Gestalt $4m + 1$ haben. Aus der Formel $7n + 1$ entsteht, nach der obigen Auseinandersetzung

$$4 \,.\, 7z + 7r + 1,$$

wobei r diejenige unter den Zahlen 0, 1, 2, 3 bedeutet, welche nach Modul 4 congruent $7(1-1) = 0$ ist. Es ist also in diesem Falle $r = 0$; folglich ergiebt die Formel $7n + 1$ für die Bestimmung der Zahlen, welche durch $4m + 1$ darstellbar sind, die Gestalt

$$4 \,.\, 7z + 1 = 28z + 1.$$

Indem man ebenso mit den Formeln

$$7n + 4, \quad 7n + 2$$

verfährt, erhält man beziehungsweise

$$4 \,.\, 7z + 7r + 4, \quad 4 \,.\, 7z + 7r' + 2,$$

wobei r, r' diejenigen aus den Zahlen 0, 1, 2, 3 bedeuten, welche nach Modul 4 beziehungsweise congruent $7(1-4) = -21$; $7(1-2) = -7$ sind. Man erhält also $r = 3$; $r' = 1$, folglich ergeben die Formeln $7n + 4$, $7n + 2$ für die Bildung von Zahlen von der ausschliesslichen Gestalt $4m + 1$ die Formeln

$$4 \,.\, 7z + 3 \,.\, 7 + 4; \quad 4 \,.\, 7z + 7 + 2,$$

oder

$$28z + 25; \quad 28z + 9.$$

Somit erhalten wir alle Zahlen von der Gestalt $4m + 1$, welche die Gleichung

$$\left(\frac{M}{7}\right) = 1$$

befriedigen, welche also etwa Theiler der quadratischen Form $x^2 - 7y^2$ sein könnten, in den Formeln

$$28z + 1; \quad 28z + 9; \quad 28z + 25.$$

Was nun die Theiler der Form $x^2 - 7y^2$, welche die Gestalt $4m + 3$ haben sollen, betrifft, so werden dieselben zunächst, nach Lehrsatz 54 der Gleichung

$$\left(\frac{M}{7}\right) = -1$$

zu genügen haben.

Wir finden aber die Lösungen dieser Gleichung, indem wir, nach § 28, aus der Reihe der Zahlen

$$1, \quad 2, \quad 3, \quad 4, \quad 5, \quad 6,$$

diejenigen fortlassen, welche als Reste bei der Division von

$$1^2, \quad 2^2, \quad 3^2$$

durch 7 erhalten werden. Wir haben also in unserem Falle 1, 2, 4 wegzulassen und es bleiben die Zahlen 3, 5, 6 zurück, welche die Lösungen von

$$\left(\frac{M}{7}\right) = -1$$

in der Gestalt

$$7n + 3, \quad 7n + 5, \quad 7n + 6$$

liefern.

Indem wir diese Lösungen so transformiren, dass aus denselben nur Zahlen von der Gestalt $4m + 3$ sich ergeben möchten, erhalten wir:

$$4 \,.\, 7z + 7r + 3; \quad 4 \,.\, 7z + 7r_1 + 5; \quad 4 \,.\, 7z + 7r_2 + 6,$$

wobei r, r_1, r_2, diejenigen aus den Zahlen 0, 1, 2, 3 bedeuten, welche nach Modul 4 beziehungsweise

$$7(3-3) = 0; \quad 7(3-5) = -14; \quad 7(3-6) = -21$$

congruent sind. Setzt man nun die sich daraus ergebenden Werthe

$$r = 0; \quad r_1 = 2; \quad r_2 = 3$$

in die letzten Formeln ein, so erhält man

$$4 \,.\, 7z + 7 \,.\, 0 + 3; \quad 4 \,.\, 7z + 7 \,.\, 2 + 5; \quad 4 \,.\, 7z + 7 \,.\, 3 + 6,$$

also:

$$28z + 3, \quad 28z + 19; \quad 28z + 27.$$

Stellen wir nun die Resultate zusammen, so haben wir alle Theiler der quadratischen Form $x^2 - 7y^2$, welche die Gestalt $4m + 1$ haben, in den Formeln

$$28z + 1; \quad 28z + 9; \quad 28z + 25;$$

während diejenigen Theiler der genannten Form, welche die Gestalt $4m + 3$ haben, in den Formeln



$$28z + 3; \quad 28z + 19; \quad 28z + 27$$

dargestellt sind.

Wir haben bis jetzt gezeigt wie man die Theiler einer Form $x^2 \pm Ay^2$ bestimmen kann, *wenn A eine von 2 verschiedene* Primzahl ist; nunmehr wollen wir zeigen, wie man die Theiler einer solchen Form, *wenn $A = 2$ ist*, finden kann.

Wir beweisen zu dem Ende folgenden Lehrsatz.

55. *Lehrsatz. Alle ungeraden Theiler der quadratischen Form $x^2 + 2y^2$ haben die Gestalt*

$$8m + 1, \quad \text{oder} \quad 8m + 3;$$

alle ungeraden Theiler der Form

$$x^2 - 2y^2$$

haben die Gestalt

$$8m + 1, \quad \text{oder} \quad 8m - 1.$$

Beweis. Ist M ein Theiler von $x^2 + 2y^2$, so wird

$$x^2 + 2y^2 \equiv 0 \pmod{M}.$$

Diese Congruenz setzt aber (nach Lehrs. 50) die Existenz von

$$u^2 + 2 \equiv 0 \pmod{M}$$

voraus, folglich auch die Existenz der Gleichungen

$$\left(\frac{-2}{\alpha}\right) = 1; \quad \left(\frac{-2}{\beta}\right) = 1; \quad \left(\frac{-2}{\gamma}\right) = 1; \quad \ldots.,$$

wobei $\alpha, \beta, \gamma, \ldots.$ die in M enthaltenen Primzahlfactoren bedeuten.

Wir haben nun die Frage zu beantworten: wie müssen die Primzahlen $\alpha, \beta, \gamma, \ldots.$ beschaffen sein, damit diese Gleichungen befriedigt werden?

Nach den Eigenschaften des Legendre'schen Symbols $\left(\frac{q}{p}\right)$ finden wir nun

$$\left(\frac{-2}{\alpha}\right) = \left(\frac{2}{\alpha}\right)(-1)^{\frac{\alpha-1}{2}},$$

während $\left(\frac{2}{\alpha}\right)$, wie wir (§ 26, Zus. II) gesehen haben, den Werth

$$\left(\frac{2}{\alpha}\right) = (-1)^{\frac{\alpha^2-1}{8}}$$

besitzt. Folglich ist

$$\left(\frac{-2}{\alpha}\right) = (-1)^{\frac{\alpha-1}{2}+\frac{\alpha^2-1}{8}} = (-1)^{\frac{\alpha^2+4\alpha-5}{8}}.$$

Setzt man darin hintereinander die überhaupt nur möglichen Werthe

$\alpha = 8m+1$; $\alpha = 8m+3$; $\alpha = 8m+5$; $\alpha = 8m+7$,

so erhält man:

$$\left(\frac{-2}{8m+1}\right) = 1; \quad \left(\frac{-2}{8m+3}\right) = 1;$$

$$\left(\frac{-2}{8m+5}\right) = -1; \quad \left(\frac{-2}{8m+7}\right) = -1.$$

Folglich ist es für die Möglichkeit der Gleichungen

$$\left(\frac{-2}{\alpha}\right) = 1; \quad \left(\frac{-2}{\beta}\right) = 1; \quad \left(\frac{-2}{\gamma}\right) = 1; \; \ldots\ldots$$

nothwendig, dass α, β, γ, ... die Gestalt

$$8m+1, \quad \text{oder} \quad 8m+3$$

haben müssen.

Daher wird M, als Product der Factoren α, β, γ, ... die Gestalt

$$(8m+1)\,(8m'+1)\,(8m''+1)\ldots\ldots(8m_1+3)\,(8m_2+3)\ldots\ldots(8m_\sigma+3)$$

haben.

Indem man sich nun dieses Product ausgerechnet denkt und alle mit 8 multiplicirten Glieder vereinigt, erhält man

$$M = 8P + 3^\sigma.$$

Ist σ eine gerade Zahl, so ist $3^\sigma \equiv 1$ (mod. 8), weil $3^2 \equiv 1$ (mod. 8) ist. Ist dagegen σ ungerade, so wird die

zur Potenz $\frac{\sigma-1}{2}$ erhobene und dann mit 3 multiplicirte Congruenz $3^2 \equiv 1 \pmod{8}$ die Congruenz

$$3^\sigma \equiv 3 \pmod{8}$$

ergeben.

Somit ist 3^σ nach Modul 8 congruent entweder 1 oder 3. Daraus folgt, dass 3^σ entweder die Gestalt $8N+1$, oder $8N+3$ hat und daher muss die Zahl M, welche durch

$$M = 8P + 3^\sigma$$

definirt ist,

$$\text{entweder} \quad 8(P+N)+1, \quad \text{oder} \quad 8(P+N)+3$$

sein [*)]. Dadurch ist der erste Theil des Lehrsatzes bewiesen.

Wir gehen nun zum zweiten Theile des Lehrsatzes über.

Ist M ein Theiler der quadratischen Form x^2-2y^2, so findet die Congruenz statt

$$x^2-2y^2 \equiv 0 \pmod{M}.$$

[*) Auch hier könnte es scheinen einer anschaulichen Ergänzung des Beweises für $M = \alpha^m \beta^n \gamma^r \ldots$ zu bedürfen. Indess kann vielleicht folgende Bemerkung den ganzen Beweis etwas übersichtlicher machen.

Die Zahlen von der Gestalt $8m+1$ und $8m+3$ haben folgende Eigenthümlichkeit:

I. $(8m+1)(8m'+1) = 8l+1$; II. $(8m_1+3)(8m_2+3) = 8m+1$;
III. $(8m_1+1)(8m_2+3) = 8n+3$.

D. h. *zwei Zahlen von gleicher Art liefern, mit einander multiplicirt, ein Product von der Gestalt* $8m+1$; *zwei Factoren von ungleicher Art liefern dagegen ein Product von der Gestalt* $8m+3$. Daraus folgt unmittelbar, dass *ein Product von beliebig vielen Factoren beiderlei Arten immer von der Gestalt*

$$8m+1, \quad \text{oder} \quad 8m+3$$

sein wird, jenachdem die Anzahl der darin auftretenden Factoren von der Gestalt $8m+3$ *eine gerade, oder ungerade ist.* Hiermit ist der erste Theil des Satzes nicht allein bewiesen, sondern ist auch zugleich ein Kriterium gegeben, wann der eine oder der andere der Fälle eintritt.]

Diese Congruenz setzt das Bestehen der Congruenz

$$u^2 - 2 \equiv 0 \pmod{M}$$

voraus, folglich die gleichzeitige Existenz der Gleichungen

$$\left(\frac{2}{\alpha}\right) = 1; \ \left(\frac{2}{\beta}\right) = 1; \ \left(\frac{2}{\gamma}\right) = 1; \ \ldots .$$

wenn $\alpha, \beta, \gamma, \ldots$ die in M auftretenden Primzahlfactoren bedeuten. Nach Lehrsatz 32 folgt aus diesen Gleichungen, dass $\alpha, \beta, \gamma, \ldots$ die Gestalt

$$8m + 1, \quad \text{oder} \quad 8m - 1$$

haben müssen; folglich wird M als Product $\alpha \beta \gamma \ldots$ die Gestalt

$$(8m' + 1)\ (8m'' + 1) \ldots . (8m_1 - 1)\ (8m_2 - 1) \ldots .$$

haben.

In dem ausgerechneten Producte tritt aber ausser den Gliedern, welche Vielfache von 8 sind, entweder $+1$, oder -1 noch hinzu; folglich muss M [*)] entweder die Gestalt $8m + 1$, oder $8m - 1$ besitzen, was zu beweisen war.

Nachdem wir nun gezeigt haben, wie man die linearen Theiler einer quadratischen Form $x^2 \pm Ay^2$ bestimmt, sowohl wenn A eine ungerade Primzahl, als auch wenn $A = 2$ ist, so bleibt uns noch übrig dasselbe für den allgemeinen Fall, wenn A eine zusammengesetzte Zahl ist, zu zeigen.

In diesem Falle lassen sich aber die linearen Theiler der quadratischen Form $x^2 \pm Ay^2$ am bequemsten aus den quadratischen Theilern derselben Form herleiten, zu deren Untersuchung wir nunmehr übergehen wollen.

[*) Auch die Zahlen von der Gestalt $8m + 1$ und $8m - 1$ haben genau die analoge Eigenthümlichkeit, dass ein Product beliebig vieler Factoren beiderlei Arten die Gestalt $8m + 1$, oder $8m - 1$ hat, jenachdem die Anzahl der Factoren $8m - 1$ gerade, oder ungerade ist.]

§ 45. Ueber die Eigenschaften allgemeiner quadratischer Formen.

Einen Ausdruck von der allgemeinen Gestalt

$$au^2 + 2buv + cv^2,$$

in welchem man unter a, b, c irgend welche, aber jedesmal als bestimmt gegeben gedachte, während man dagegen unter u, v unbestimmte ganze Zahlen versteht, nennt man „*eine allgemeine quadratische*", oder schlechtweg „*eine quadratische Form.*"

[Indem man für u, v irgend welche Zahlen setzt, erhält man jedesmal eine bestimmte Zahl durch die Form dargestellt. Die Gesammtheit aller Zahlen, welche auf diese Weise durch alle möglichen Werthe von u, v durch die Form überhaupt erhalten werden können, gruppirt man als „*die durch die gegebene Form darstellbaren Zahlen.*"]

Zwei quadratische Formen

$$au^2 + 2b\,uv + c\,v^2,$$
$$a'u^2 + 2b'uv + c'v^2,$$

welche die Eigenschaft haben, dass alle Zahlen, welche mittels einer der Formen, durch Einsetzung aller möglichen Zahlen für u, v, darstellbar sind, auch durch die andere, wenn auch durch andere Anordnung der Werthe von u, v, dargestellt werden können, wollen wir *identische Formen* nennen und werden solche gegenseitig durch einander ersetzen.

So z. B. sind die beiden Formen

$$au^2 + 2buv + cv^2,$$
$$au^2 - 2buv + cv^2,$$

welche sich von einander nur durch das Vorzeichen des Coefficienten von uv unterscheiden, auch als einander identisch zu betrachten; denn die Zahlen, welche durch die eine Form für $u = \alpha$, $v = \beta$ dargestellt werden, werden durch die andere für $u = -\alpha$, $v = \beta$ dargestellt.

Daraus geht hervor, dass das Vorzeichen des Coefficienten b in einer Form



$$au^2 + 2buv + cv^2$$

beliebig geändert werden darf, so dass man diesen Coefficienten nöthigenfalls in eine positive Zahl verwandeln kann; wir werden ihn daher immer positiv voraussetzen.

Die Zahl $b^2 - ac$ wollen wir, nach Gauss, ihrer wichtigen Rolle wegen, welche wir bald kennen lernen werden, die *Determinante* der quadratischen Form

$$au^2 + 2buv + cv^2$$

nennen.

So ist z. B. für die Form $3u^2 + 10uv + 7v^2$ die Determinante $5^2 - 3 . 7 = 4$; von $3u^2 + 10uv - 7v^2$ ist die Determinante $5^2 + 3 . 7 = 46$.

Zwei Formen, welche gleiche Determinante haben, wollen wir *ähnliche* Formen nennen.

So z. B. werden die Formen

$$3u^2 + 10uv + 7v^2,$$
$$3u^2 + 2uv - v^2$$

ähnliche Formen sein, weil die Determinante der erstern $5^2 - 3 . 7 = 4$ und die der letzteren $1^2 + 3 . 1 = 4$.

Sind wir nun so wegen der Benennung übereingekommen, so wollen wir einen Lehrsatz beweisen, welcher, seiner Anwendbarkeit willen, sehr wichtig ist.

56. *Lehrsatz. Eine Form*

$$au^2 + 2buv + cv^2,$$

in welcher der Coefficient $2b$ von uv entweder a, oder c übertrifft, kann immer in eine andere, ihr ähnliche, Form

$$a'u^2 + 2b'uv + c'v^2$$

transformirt werden, in welcher $2b'$ weder a', noch c' übertreffen wird. (*)

Beweis. Wir wollen zunächst zeigen, wie man eine Form

$$au^2 + 2buv + cv^2,$$

(*) Wir verstehen hier das *Uebertreffen* in Bezug auf die Zahlenwerthe von a, b, c, a', b', c', ohne auf die Vorzeichen dieser Zahlen zu achten.

in welcher $2b > a$, oder $2b > c$ in eine andere Form

$$a_0 u^2 + 2b_0 uv + c_0 v^2$$

transformiren kann, welche letztere der ursprünglichen Form ähnlich ist und dabei der Zahlwerth von b_0 kleiner als der von b wird. Da nun die Verkleinerung des Zahlwerthes einer Zahl nicht über Null hinausgehen kann, so werden wir bei fortfahrender Verkleinerung von b einmal zu einer Form $a'u^2 + 2b'uv + c'v^2$ gelangen müssen, in welcher eine weitere Verkleinerung von b' nicht mehr möglich ist; es wird dann folglich weder $2b' > a'$, noch $2b' > c'$ möglich sein.

Um die Form $au^2 + 2buv + cv^2$ in $a_0 u^2 + 2b_0 uv + c_0 v^2$ so zu transformiren, dass b_0 kleiner als b werde, mag a die kleinere der beiden Zahlen a, c sein (falls a, c einander gleich sind, kann jede von ihnen ohne Unterschied gewählt werden) und mag diejenige ganze Zahl, welche von $\frac{b}{a}$ nicht um mehr als um $\frac{1}{2}$ differirt, mit m bezeichnet werden. Man wird offenbar für m diejenige ganze Zahl zu setzen haben, welche durch die Division von b durch a erhalten wird, falls der verbleibende Rest nicht grösser als $\frac{1}{2}a$ wird; im entgegengesetzten Falle wird man für m die um 1 vermehrte Zahl setzen, welche bei der Division von b durch a erhalten wird. Setzen wir nun in $au^2 + 2buv + cv^2$ für u den Werth aus

$$u + mv = U$$

ein, so erhalten wir

$$a(U - mv)^2 + 2b(U - mv)v + cv^2,$$

oder

$$aU^2 + 2(b - am)Uv + (c - 2bm + am^2)v^2.$$

Man kann sich leicht überzeugen, dass diese Form der ursprünglichen $au^2 + 2buv + cv^2$ ähnlich ist und, dass der Coefficient von Uv kleiner als $2b$ wird. Denn die Determinante der transformirten Form ist

$$(b - am)^2 - a(c - 2bm + am^2) = b^2 - ac,$$

also gleich der Determinante der ursprünglichen Form.

Andererseits wird

$$2(b-am) = 2a\left(\frac{b}{a}-m\right),$$

da $\left(\frac{b}{a}-m\right)$, nach Voraussetzung $\frac{1}{2}$ nicht übertrifft, eine Zahl sein, welche a nicht übertreffen kann, folglich kleiner als $2b$ sein muss; weil wir ja von einer Form

$$au^2 + 2buv + cv^2$$

handeln, in welcher $2b$ eine der Zahlen a, oder c übertrifft und dabei haben wir a gleich c, oder kleiner als c angenommen.

Folglich wird wirklich der mittlere Coëfficient der erhaltenen Form

$$aU^2 + 2(b-am)\,Uv + (c-2bm+am^2)\,v^2$$

kleiner sein als der entsprechende Coëfficient in der ursprünglichen Form

$$au^2 + 2buv + cv^2.$$

Uebertrifft der mittlere Coëfficient der transformirten Form einen der Coëfficienten ihrer äussern Glieder, so werden wir auch diese Form vom Neuen ebenso transformiren, wie wir die ursprüngliche

$$au^2 + 2buv + cv^2$$

transformirt haben und werden solche Transformationen solange wiederholen, bis wir zu einer Form gelangen, bei welcher eine derartige Transformation nicht weiter möglich ist; der mittlere Coëfficient dieser letzten Form wird also keinen der äussern Coëfficienten übertreffen.

[Man braucht kaum zu bemerken, dass die Anzahl der dabei nöthigen Transformationen immer eine *endliche* sein wird, da der mittlere Coëfficient, der als *endliche* ganze Zahl vorausgesetzt war, durch jede Transformation offenbar immer um eine ganze Zahl kleiner wird und unter Null nicht herabsinken kann, weil nach obiger Anmerkung es sich hier immer um das Kleinerwerden des Zahlwerthes, ohne Rücksicht auf das Vorzeichen, handelt.]

Beispiel. Es mag die Form

$$3u^2 + 10uv + 6v^2$$

gegeben sein, deren mittlerer Coëfficient beide äusseren Coëfficienten übertrifft und deren kleinster Coëfficient 3 ist.

Um diese Form zu transformiren, suchen wir diejenige ganze Zahl, die von $\frac{5}{3}$ nicht um mehr als $\frac{1}{2}$ differirt. Diese Zahl ist offenbar 2 und wir setzen daher

$$u + 2v = U.$$

Indem wir daraus den Werth von u in die gegebene Form einsetzen, erhalten wir

$$3(U-2v)^2 + 10(U-2v)v + 6v^2,$$

oder, ausgerechnet und nach U und v geordnet:

$$3U^2 - 2Uv - 2v^2.$$

In dieser Form übertrifft der mittlere Coëfficient keinen der äusseren Coëfficienten; sonst würden wir vom Neuen transformiren.

Mit Hülfe des ebenbewiesenen Lehrsatzes sind wir nun im Stande folgende Lehrsätze zu beweisen.

57. *Lehrsatz. Ist die Determinante einer Form*

$$au^2 + 2buv + cv^2$$

eine positive Zahl D, so kann die Form auf eine solche

$$a_1u^2 + 2b_1uv - c_1v^2$$

gebracht werden, wobei in

$$a_1c_1 + b_1^2 = D$$

die Zahlen a_1, c_1, positiv und nicht kleiner als $2b_1$, während b_1 nicht grösser als $\sqrt{\frac{D}{5}}$ ist.

Beweis. Nach dem vorhergehenden Lehrsatze kann die Form $au^2 + 2buv + cv^2$ in eine

$$a_1u^2 + 2b_1uv + c_0v^2$$

transformirt werden, in welcher $2b_1$ im Zahlwerth weder a_1, noch c_0 übertrifft; dabei wird die Determinante der transformirten Form, welche der ursprünglichen ähnlich sein soll, denselben Werth D haben; folglich ist

$$b_1^2 - a_1 c_0 = D.$$

Ist aber, wie wir in unserem Lehrsatze voraussetzen, $D > 0$, so sagt die letzte Gleichung aus, dass die Differenz

$$b_1^2 - a_1 c_0$$

eine positive Zahl ist, was nicht möglich sein kann, wenn a_1 und c_0 gleiches Vorzeichen haben; weil dann das Product $a_1 c_0$ eine positive Zahl wird, welche b_1^2 übertrifft, da der Zahlwerth von a_1 und c_0 nicht kleiner als $2b_1$ war.

Somit müssen die äussern Coëfficienten der Form

$$a_1 u^2 + 2b_1 uv + c_0 v^2$$

entgegengesetzte Vorzeichen haben. Nehmen wir an, das Glied $a_1 u^2$ sei dasjenige, welches das Vorzeichen $+$ hat und somit hat $c_0 v^2$ das Vorzeichen $-$. Bezeichnen wir mit c_1 den Zahlwerth von c_0, so erhalten wir $c_0 = -c_1$, wodurch die Form

$$a_1 u^2 + 2b_1 uv + c_0 v^2$$

mit der Determinante

$$b_1^2 - a_1 c_0 = D$$

in die Form

$$a_1 u^2 + 2b_1 uv - c_1 v^2$$

mit der Determinante

$$b_1^2 + a_1 c_1 = D$$

übergeht. Nach der Beschaffenheit der Coëfficienten

$$a_1, \quad b_1, \quad c_1$$

ist aber

$$a_1 \text{ nicht } < 2b_1, \quad c_1 \text{ nicht } < 2b_1$$

wodurch aus der Gleichung

$$b_1^2 + a_1 c_1 = D$$

sich ergiebt:

$$D \text{ nicht } < b_1^2 + 2b_1 . 2b_1; \quad \text{d. h. } D \text{ nicht } < 5b_1^2,$$

folglich

$$b_1 \text{ nicht } > \sqrt{\frac{D}{5}}.$$

Die Coëfficienten der Form

$$a_1 u^2 + 2 b_1 uv - c_1 v^2,$$

welche durch Transformation aus der gegebenen Form

$$au^2 + 2buv + cv^2$$

hervorgegangen ist, unterliegen also gleichzeitig den Bedingungen

$$b_1^2 + a_1 c_1 = D; \quad a_1 \text{ nicht } < 2b_1; \quad c_1 \text{ nicht } < 2b_1$$

und

$$b_1 \text{ nicht } > \sqrt{\frac{D}{5}},$$

was zu beweisen war.

58. *Lehrsatz. Ist die Determinante einer Form*

$$au^2 + 2buv + cv^2$$

eine negative Zahl $-D$, *so kann die Form auf eine solche*

$$a_1 u^2 + 2b_1 uv + c_1 v^2$$

gebracht werden, wobei in

$$a_1 c_1 - b_1^2 = D$$

a_1 *und* c_1 *gleiches Vorzeichen haben und nicht kleiner als* $2 b_1$ *sind, während* b_1 *die Grösse*

$$\sqrt{\frac{D}{3}}$$

nicht übertrifft.

Beweis. Wir haben bereits gesehen, dass die Form

$$au^2 + 2buv + cv^2$$

in eine andere

$$a_1 u^2 + 2b_1 uv + c_1 v^2$$

transformirt werden kann, wobei $2b_1$, weder a_1, noch c_1 übertreffen wird; dabei hat die Determinante der transformirten Form, da letztere der ursprünglichen ähnlich ist,

denselben Werth $-D$ wie die Determinante der ursprünglichen Form; folglich ist

$$b_1^2 - a_1 c_1 = -D.$$

Diese Gleichung, in welcher D eine positive Zahl ist, setzt aber voraus, dass a_1 und c_1 gleiches Vorzeichen haben. Indem wir nun berücksichtigen, dass weder a_1 noch c_1 kleineren Zahlwerth als $2b_1$ besitzen, leiten wir aus der letztgenannten Gleichung die Bedingung

$$2b_1 . 2b_1 - b_1^2 \text{ nicht } > D,$$

oder

$$3b_1^2 \text{ nicht } > D$$

her; es ist also

$$b_1 \text{ nicht } > \sqrt{\frac{D}{3}}.$$

Nachdem wir den Lehrsatz bewiesen haben, constatiren wir noch folgenden

Zusatz. In dem vorliegenden Falle kann die Form

$$a_1 u^2 + 2b_1 uv + c_1 v^2$$

nur dann eine positive Zahl darstellen, wenn a_1 positiv ist.

Denn der Ausdruck $a_1 u^2 + 2b_1 uv + c_1 v^2$ kann so geschrieben werden:

$$a_1 \left(u^2 + 2\frac{b_1}{a_1} uv + \frac{c_1}{a_1} v^2\right),$$

also auch

$$a_1 \left[\left(u + \frac{b_1}{a_1} v\right)^2 + \frac{a_1 c_1 - b_1^2}{a_1^2} v^2\right],$$

welcher Ausdruck, auf Grund von

$$b_1^2 - a_1 c_1 = -D,$$

in

$$a_1 \left[\left(u + \frac{b_1}{a_1} v\right)^2 + \frac{D}{a_1^2} v^2\right]$$

übergeht.

Ist nun a_1 negativ, so kann dieser Ausdruck keinen positiven Werth annehmen, da $D > 0$ und die Quadrate $\left(u + \frac{b_1}{a_1} v\right)^2$, $\left(\frac{v}{a_1}\right)^2$ keine negativen Werthe zulassen.

§ 46. Ueber die Darstellbarkeit der Theiler von $x^2 \pm Ay^2$ durch quadratische Formen.

Nachdem wir die Haupteigenschaften der quadratischen Formen, welche wir in der Folge nothwendig brauchen, gezeigt haben, wenden wir uns wiederum zu den Theilern der Form von der Gestalt $x^2 \pm Ay^2$ und wollen folgenden Lehrsatz beweisen.

59. *Lehrsatz. Jeder Theiler einer Form*

$$x^2 - dy^2$$

kann immer durch eine quadratische Form dargestellt werden, welche die Determinante d besitzt.

Beweis. Sei M ein Theiler der Form $x^2 - dy^2$ und Q mag den Quotienten bei der Division von $x^2 - dy^2$ durch M darstellen; man erhält dann

$$x^2 - dy^2 = M \,.\, Q.$$

Es müssen hier y und Q Zahlen sein, welche relativ prim zu einander sind; weil, nach dieser Gleichung jede Primzahl, welche zugleich y und Q theilen würde, zugleich auch x theilen müsste. Letzteres ist aber unmöglich, da wir in der Form $x^2 - dy^2$ immer x und y als relativ prim zu einander voraussetzen.

Ist aber y relativ prim zu Q, so wird die Congruenz

$$yt \equiv x \pmod{Q}$$

eine Lösung besitzen; es wird sich also immer eine Zahl t derart bestimmen lassen, dass die Differenz $yt - x$ durch Q theilbar werde. Setzten wir den Quotienten dieser Division gleich u, so erhalten wir

$$\frac{yt - x}{Q} = u,$$

woraus sich ergiebt

$$x = yt - uQ.$$

Setzt man diesen Werth von x in die obige Gleichung

$$x^2 - dy^2 = MQ$$

ein, so erhält man

$$(yt-uQ)^2-dy^2 = MQ,$$

oder

$$Q^2u^2-2Qytu+(t^2-d)y^2 = MQ.$$

Nach Division durch Q erhält man aus dieser Gleichung

$$M = Qu^2-2ytu+\frac{t^2-d}{Q}y^2,$$

wobei t^2-d durch Q theilbar sein muss, weil diese Gleichung die Theilbarkeit von $(t^2-d)y^2$ durch Q offenbar voraussetzt, während y relativ prim zu Q ist.

Aus dieser Gleichung ersehen wir, dass der Theiler M von x^2-dy^2 durch die quadratische Form

$$M = Qu^2-2tuy+\frac{t^2-d}{Q}y^2$$

dargestellt ist, deren Coëfficienten

$$Q, \quad -2t, \quad \frac{t^2-d}{Q}$$

sind und somit ist die Determinante dieser quadratischen Form

$$t^2-Q\cdot\frac{t^2-d}{Q} = d,$$

was zu beweisen war.

Mit Hülfe dieses Lehrsatzes und Berücksichtigung der oben bewiesenen Eigenschaften der quadratischen Formen kann man leicht folgende Lehrsätze beweisen.

60. *Lehrsatz.* *Ein Theiler von x^2-Dy^2 kann, wenn $D>0$, durch eine Form*

$$au^2+2buv-cv^2$$

dargestellt werden, in welcher

$$b^2+ac = D,$$

die Zahlen a, c positiv und nicht kleiner als $2b$ sind, während b die Zahl

$$\sqrt{\frac{D}{5}}$$

nicht übertrifft.

Beweis. Nach dem vorhergehenden Lehrsatze kann man jeden Theiler von $x^2 - Dy^2$ durch eine Form

$$au^2 + 2buv + cv^2$$

darstellen, deren Determinante

$$b^2 - ac = D$$

ist. Nun kann eine solche Form, nach Lehrsatz 57, immer auf die Gestalt

$$au^2 + 2buv - cv^2$$

gebracht werden, in welcher a, b, c der Gleichung

$$b^2 + ac = D$$

genügen, während die Zahlen a, c positiv und nicht kleiner als $2b$ sind und b nicht die Zahl $\sqrt{\frac{D}{5}}$ übertrifft. Somit ist unser Lehrsatz bewiesen.

61. *Lehrsatz. Ein Theiler von $x^2 + Dy^2$ kann, wenn $D > 0$, durch eine Form*

$$au^2 + 2buv + cv^2$$

dargestellt werden, in welcher

$$ac - b^2 = D,$$

die Zahlen a, c positiv und nicht kleiner als $2b$, während b die Zahl

$$\sqrt{\frac{D}{3}}$$

nicht übertrifft.

Beweis. Nach Lehrsatz 59, kann jeder Theiler von

$$x^2 + Dy^2$$

durch eine quadratische Form

$$au^2 + 2buv + cv^2$$

dargestellt werden, deren Determinante $-D$ ist. Eine solche Form kann aber, nach Lehrsatz 58, dahin gebracht werden, dass zugleich mit der Bedingung $ac - b^2 = D$ auch die Bedingungen erfüllt werden, dass der Zahlwerth von a, c nicht kleiner als $2b$, während b die Zahl $\sqrt{\frac{D}{3}}$ nicht übertrifft. Dabei müssen a, c nach demselben Lehr-

satze, gleiches Vorzeichen haben; dieses Vorzeichen kann aber in unserem Falle nicht — sein, da dann die Form

$$au^2 + 2buv + cv^2,$$

nach Zusatz zu Lehrs. 58, keine positiven Werthe annehmen könnte. Somit ist unser Lehrsatz bewiesen.

Auf Grund der eben bewiesenen Lehrsätze kann man nun zeigen durch welche quadratische Formen *alle* Theiler einer gegebenen Form

$$x^2 \pm Dy^2$$

dargestellt werden können. Einige Beispiele sollen dieses näher erläutern.

Beispiele. 1) Es sei die Form $x^2 + y^2$ gegeben. Nach Lehrsatz 61 werden die Theiler dieser Form durch quadratische Formen von der Gestalt

$$au^2 + 2buv + cv^2$$

dargestellt werden, wobei $ac - b^2 = 1$, während a und c positiv und nicht kleiner als $2b$ und b nicht grösser als $\sqrt{\frac{1}{3}}$. Aus der letzten Bedingung folgt $b = 0$ und aus der Gleichung $ac - b^2 = 1$ ergiebt sich dann $ac = 1$, woraus für a und c, welche beide > 0 sein müssen, folgt

$$a = 1; \quad c = 1.$$

Folglich erhalten wir den Satz:

Alle Theiler der Form $x^2 + y^2$, werden durch die Form $u^2 + v^2$ dargestellt.

---

2) Es sei die gegebene Form $x^2 + 2y^2$. Auf Grund desselben Lehrsatzes 61 können die Theiler dieser Form durch Formeu von der Gestalt

$$au^2 + 2buv + cv^2$$

dargestellt werden, wobei $ac - b^2 = 2$, während a, c positiv und nicht kleiner als $2b$ und b nicht grösser als $\sqrt{\frac{2}{3}}$.

Aus der Bedingung b nicht $> \sqrt{\frac{2}{3}}$ folgt $b = 0$;



dann geht $ac - b^2 = 2$ in $ac = 2$ über. Da nun a, c positiv sein müssen, so kann die letzte Gleichung nur entweder für $a = 2$; $c = 1$, oder $a = 1$; $c = 2$ erfüllt werden; der ersten Annahme entspricht die Form $2u^2 + v^2$, der zweiten $u^2 + 2v^2$. Diese beiden Formen sind aber einander identisch und somit haben wir den Satz:

Alle Theiler der Form $x^2 + 2y^2$ werden durch eine Form $u^2 + 2v^2$ dargestellt.

In ganz analoger Weise beweist man folgende Sätze:

3) *Alle Theiler der Form $x^2 - y^2$ werden durch die Form $u^2 - v^2$ dargestellt.*

4) *Alle Theiler der Form $x^2 - 2y^2$ werden, entweder durch $u^2 - 2v^2$, oder durch die Form $2u^2 - v^2$ dargestellt.*

5) *Alle Theiler von $x^2 - 3y^2$ werden entweder durch $u^2 - 3v^2$ oder durch $3u^2 - v^2$ dargestellt.*

6) Als etwas complicirteres Beispiel mag die Form $x^2 - 21y^2$ dienen.

Nach Lehrsatz 60 werden die Theiler dieser Form durch quadratische Formen von der Gestalt

$$au^2 + 2buv - cv^2$$

dargestellt, in welcher a, b, c positiv und die Bedingungen

$$b \text{ nicht} > \sqrt{\frac{21}{5}}; \quad ac + b^2 = 21$$

erfüllen.

Die erste Bedingung definirt alle möglichen Werthe von b; es kann nämlich b nur einen der drei Werthe

$$b = 0, 1, 2$$

haben. Indem man nun in $ac + b^2 = 21$ für b nach einander die drei möglichen Werthe setzt und berücksichtigt, dass a, c grösser als 0 und nicht kleiner als $2b$ sind, findet man alle möglichen Werthe, welche a, b, c in derjenigen

Form $au^2 + 2buv - cv^2$ annehmen können, welche die Theiler von $x^2 - 21y^2$ darstellen soll.

Setzen wir z. B. zunächst $b = 0$, so folgt $ac = 21$, welche Bedingung nur durch folgende Werthepaare erfüllt werden kann:

$$\begin{array}{c|c|c|c} a = 1 & a = 3 & a = 7 & a = 21 \\ c = 21 & c = 7 & c = 3 & c = 1, \end{array}$$

welche alle zugleich die Bedingungen

$$a \text{ und } c > 0 \text{ und nicht } < 2b, \text{ wo } b = 0 \text{ ist,}$$

erfüllen.

Setzen wir $b = 1$, so erhalten wir $ac + 1 = 21$, also $ac = 20$, woraus die Werthepaare für a, c

$$\begin{array}{c|c|c|c|c|c} a = 1 & a = 2 & a = 4 & a = 5 & a = 10 & a = 20 \\ c = 20 & c = 10 & c = 5 & c = 4 & c = 2 & c = 1 \end{array}$$

folgen.

Erstes und letztes Werthepaar genügen aber nicht der Bedingung a, c nicht $< 2b$, da $b = 1$ ist. Folglich bleiben für $b = 1$ nur die Möglichkeiten

$$\begin{array}{c|c|c|c} a = 2 & a = 4 & a = 5 & a = 10 \\ c = 10 & c = 5 & c = 4 & c = 2. \end{array}$$

Setzen wir endlich $b = 2$, so erhalten wir $ac = 17$, folglich entweder $a = 1$; $c = 17$, oder $a = 17$; $c = 1$. Beide Werthepaare sind aber unmöglich, da hier $2b = 4$ in der ersten Annahme a, in der zweiten c übertreffen würde.

Somit müssen alle Theiler von $x^2 - 21y^2$ durch irgend welche der folgenden Formen sich darstellen lassen:

$$u^2 - 21v^2; \quad 3u^2 - 7v^2; \quad 7u^2 - 3v^2; \quad 21u^2 - v^2;$$

$$2u^2 + 2uv - 10v^2; \quad 4u^2 + 2uv - 5v^2; \quad 5u^2 + 2uv - 4v^2;$$
$$10u^2 + 2uv - 2v^2.$$

Da die erste und die letzte in der zweiten Reihe: $2u^2 + 2uv - 10v^2$; $10u^2 + 2uv - 2v^2$ nur gerade Zahlen darstellen können, so sieht man zugleich, dass alle ungeraden Theiler von $x^2 - 21y^2$ nur durch die Formen

$$u^2 - 21v^2, \quad 3u^2 - 7v^2, \quad 7u^2 - 3v^2, \quad 21u^2 - v^2;$$
$$4u^2 + 2uv - 5v^2, \quad 5u^2 + 2uv - 4v^2$$

dargestellt werden können.

7) Es sei die Form $x^2 + 26y^2$ gegeben.

Die Theiler dieser Form werden, nach Lehrsatz 61, durch quadratische Formen

$$au^2 + 2buv + cv^2$$

dargestellt, wobei

$$b \text{ nicht } > \sqrt{\frac{26}{3}}; \quad ac - b^2 = 26; \quad a \text{ und } c \text{ nicht } < 2b.$$

Die erste Ungleichung zeigt, dass b nur einen der drei Werthe

$$b = 0, 1, 2$$

haben kann.

Setzt man $b = 0$, so ergeben sich für a, c die Bedingungen

$$ac = 26; \quad a \text{ und } c \text{ nicht } < 0.$$

Diese Bedingungen führen auf eine der Annahmen:

$a = 1$	$a = 2$	$a = 13$	$a = 26$
$c = 26$	$c = 13$	$c = 2$	$c = 1$,

welche die Formen

$$u^2 + 26v^2; \quad 2u^2 + 13v^2; \quad 13u^2 + 2v^2; \quad 26u^2 + v^2$$

ergeben. Von diesen sind aber die erste und die letzte unter einander, ebenso wie die beiden mittleren Formen untereinander identisch. Es bleiben also für $b = 0$ nur die zwei verschiedenen Formen

$$u^2 + 26v^2, \quad 2u^2 + 13v^2$$

möglich.

Setzt man $b = 1$, so erhält man für a, c die Bedingungen:

$$ac = 27; \quad a \text{ und } c \text{ nicht } < 2.$$

Die erste Bedingung erfüllen:

$a = 1$	$a = 3$	$a = 9$	$a = 27$
$c = 27$	$c = 9$	$c = 3$	$c = 1$.

Die erste Annahme genügt aber nicht der Bedingung

$$a \text{ nicht } < 2,$$

während die letzte Annahme der Bedingung

$$c \text{ nicht } < 2$$

nicht genügt; und es bleiben somit für $b = 1$ nur die beiden Formen

$$3u^2 + 2uv + 9v^2, \quad 9u^2 + 2uv + 3v^2$$

welche übrigens einander identisch sind.

Setzt man endlich $b = 2$, so ergiebt sich

$$ac = 30; \quad a \text{ und } c \text{ nicht } < 4.$$

Die Gleichung $ac = 30$ befriedigen die Annahmen

$$\begin{array}{c|c|c|c|c|c} a = 1 & a = 2 & a = 3 & a = 5 & a = 6 & a = 10 \\ c = 30 & c = 15 & c = 10 & c = 6 & c = 5 & c = 3 \end{array}$$

$$\begin{array}{c|c} a = 15 & a = 30 \\ c = 2 & c = 1. \end{array}$$

Indess genügen die drei ersten nicht der Bedingung

$$a \text{ nicht } < 4,$$

während die drei letzten der Bedingung

$$c \text{ nicht } < 4$$

nicht genügen. Es bleiben also nur die beiden mittelsten Annahmen möglich, welche die beiden einander identischen Formen

$$5u^2 + 4uv + 6v^2; \quad 6u^2 + 4uv + 5v^2$$

ergeben.

Somit erhält man im Ganzen nur die vier verschiedenen quadratischen Formen

$$u^2 + 26v^2; \quad 2u^2 + 13v^2$$
$$3u^2 + 2uv + 9v^2; \quad 5u^2 + 4uv + 6v^2$$

übrig, durch welche man die Theiler der Form

$$x^2 + 26y^2$$

darstellen könnte.

So haben wir auf Grund der oben bewiesenen Lehrsätze gezeigt, wie man alle quadratische Formen herleiten kann, welche die Theiler von

$$x^2 \pm Dy^2$$

darstellen.

Daraus folgert man in Bezug auf die Auflösung einer Gleichung von der Gestalt

$$ax^2 + 2bxy + cy^2 = H$$

viele merkwürdige Sätze, welche einen Gegenstand der Untersuchung für die Theorie der unbestimmten Gleichungen höheren Grades ausmachen.

Hier wollen wir die quadratischen Formen der Theiler von

$$x^2 \pm Dy^2$$

dazu benutzen, um die linearen Theiler zu bestimmen.

Wie man die linearen Theiler der quadratischen Form

$$x^2 \pm Dy^2$$

bestimmt, wenn D eine Primzahl ist, haben wir oben bereits gezeigt; jetzt wollen wir nun zeigen, wie man die Theiler derselben Form bei beliebiger Bedeutung von D finden kann, gleichviel, ob D eine Primzahl, oder zusammengesetzte Zahl ist.

Wir nehmen dabei an es sei D nicht durch das Quadrat irgend einer Zahl theilbar; eine Annahme welche jedoch keine Beschränkung der Allgemeinheit ausmacht. Denn wenn $D = D_1 k^2$ ist, so verwandelt sich die Form

$$x^2 \pm Dy^2 \text{ in } x^2 \pm D_1 k^2 y^2 = x^2 \pm D_1 (ky)^2,$$

folglich in

$$x^2 \pm D_1 y_1^2,$$

wobei $y_1 = ky$ gesetzt wurde. Auf diese Weise können wir, bei der Betrachtung der Theiler einer Form

$$x^2 \pm Dy^2,$$

die quadratischen Factoren von D weglassen; dadurch werden uns für die Untersuchung nur solche Formen $x^2 \pm Dy^2$ übrig bleiben, in welchen D nicht durch das

Quadrat irgend einer Zahl theilbar ist. Mit der Aufsuchung der Theiler solcher Formen wollen wir uns nun mehr beschäftigen.

---

§ 47. Ueber die Bestimmung der linearen Theiler einer Form $x^2 \pm Dy^2$ mit Hülfe quadratischer Formen.

Bevor wir zeigen werden, wie man aus den quadratischen Formen der Theiler die linearen Theiler herleiten kann, wollen wir noch folgende Lehrsätze in Bezug auf eine quadratische Form $au^2 + 2buv + cv^2$ beweisen.

62. *Lehrsatz. Ist die Determinante d einer quadratischen Form*

$$au^2 + 2buv + cv^2$$

eine Zahl, welche durch kein Quadrat theilbar ist, so kann man eine Zahl α derart bestimmen, dass

$$a + 2b\alpha + c\alpha^2$$

zu d relativ prim wird.

Beweis. Es sei ω der grösste gemeinsame Theiler von c und d; diese Zahl ω kann keinen quadratischen Factor enthalten, da d durch kein Quadrat theilbar ist. Aus der Bedeutung von d erhalten wir

$$b^2 - ac = d,$$

woraus folgt, dass ω, als gemeinsamer Theiler von c und d, ein Theiler von b^2 und somit, nach Lehrsatz 6, auch ein Theiler von b sein muss.

Wir wollen nun beweisen, dass

1) *eine Zahl α gefunden werden kann, für welche*

$$\frac{a\alpha + b}{\omega}$$

relativ prim zu $\frac{d}{\omega}$ wird;

2) *eine solche Zahl α macht*

$$a + 2b\alpha + c\alpha^2$$

relativ prim zu d.

Von der Richtigkeit der ersten Behauptung überzeugt man sich leicht, wenn man bemerkt, dass wenn b durch den grössten gemeinsamen Theiler ω von c und d theilbar ist, nach Lehrsatz 19, eine Zahl α gefunden werden kann, welche die Congruenz

$$c\alpha + b \equiv \omega \pmod{d}$$

befriedigt, welche die Theilbarkeit von

$$c\alpha + b - \omega$$

durch d aussagt. Bezeichnet man den Quotienten dieser Division mit N, so erhält man

$$\frac{c\alpha + b - \omega}{d} = N,$$

woraus folgt:

$$\frac{c\alpha + b}{\omega} = 1 + N\frac{d}{\omega};$$

in dieser Form ist es augenscheinlich, dass die Zahlen

$$\frac{c\alpha + b}{\omega} \text{ und } \frac{d}{\omega}$$

relativ Prim zu einander sind.

Um die zweite Behauptung zu beweisen, bemerken wir, dass der Ausdruck

$$a + 2b\alpha + c\alpha^2$$

so geschrieben werden kann:

$$\frac{\omega\left(\frac{c\alpha + b}{\omega}\right)^2 - \frac{b^2 - ac}{\omega}}{\frac{c}{\omega}}$$

und, mit Benutzung von $b^2 - ac = d$, auch so:

$$\left[\omega\left(\frac{c\alpha + b}{\omega}\right)^2 - \frac{d}{\omega}\right] : \frac{c}{\omega}.$$

Es ist nun die Zahl d als Product zweier Factoren $\frac{d}{\omega}$ und ω, also:

$$d = \frac{d}{\omega} \cdot \omega,$$

darstellbar, welche keinen gemeinsamen Theiler haben können, da d durch kein Quadrat theilbar ist. Dabei ist $\frac{d}{\omega}$, auf Grund der oben bestimmten Eigenschaft von α, relativ prim zu $\frac{c\alpha + b}{\omega}$, woraus folgt, dass weder ω, noch $\frac{d}{\omega}$ einen gemeinsamen Theiler mit

$$\omega \left(\frac{c\alpha + b}{\omega}\right)^2 - \frac{d}{\omega}$$

besitzen kann; weil die in ω enthaltenen Primzahlfactoren

Theiler von $\omega \left(\frac{c\alpha + b}{\omega}\right)^2$ und keine Theiler von $\frac{d}{\omega}$,

während die in $\frac{d}{\omega}$ enthaltenen Primzahlfactoren, umgekehrt,

Theiler von $\frac{d}{\omega}$ und keine Theiler von $\omega \left(\frac{c\alpha + b}{\omega}\right)^2$

sind. Somit ist $\omega \left(\frac{c\alpha + b}{\omega}\right)^2 - \frac{d}{\omega}$ und folglich auch

$$\frac{\omega \left(\frac{c\alpha + b}{\omega}\right)^2 - \frac{d}{\omega}}{\frac{c}{\omega}} = a + 2b\alpha + c\alpha^2$$

relativ prim sowohl zu $\frac{d}{\omega}$, als auch zu ω und daher zu ihrem Producte d, was wir beweisen wollten.

Beispiel. Wir wollen eine Zahl α finden, für welche die Zahl

$$3 + 2 \,.\, 21\alpha + 217\alpha^2$$

relativ prim wird zu

$$21^2 - 3 \,.\, 217 = -210.$$

Indem wir bemerken, dass 7 der grösste gemeinsame Theiler von 217 und 210 ist, erhalten wir für die Bestimmung von α die Bedingung, dass

$$\frac{217\alpha + 21}{7} = 31\alpha + 3 \text{ relativ prim zu } \frac{210}{7} = 30$$

werde. Dieser Bedingung kann man, wie wir gesehen haben, durch eine Lösung der Congruenz

$$217\alpha + 21 \equiv 7 \pmod{210}$$

genügen.

Indess kann man in diesem Falle, wie auch in den meisten Fällen überhaupt, die Zahl α leicht durch Probieren verschiedener Zahlen finden. So finden wir z. B. dass $\alpha = -2$ den Ausdruck $31\alpha + 3$ in eine Zahl verwandelt, welche relativ prim zu 30 ist und somit wird auch

$$3 + 2 \cdot 21\alpha + 217\alpha^2, \text{ für } \alpha = -2,$$

relativ prim zu 210.

Auf Grund des bewiesenen Lehrsatzes kann man somit für jede quadratische Form

$$au^2 + 2buv + cv^2$$

eine Zahl α finden, welche den Ausdruck

$$a + 2b\alpha + c\alpha^2$$

relativ prim zu der Determinante der Form macht. Indem wir die Zahl α so bestimmen, sind wir nun im Stande:

durch die Substitution

$$v - \alpha u = V$$

die Form

$$au^2 + 2buv + cv^2$$

in eine andere

$$(a + 2b\alpha + c\alpha^2)u^2 + 2(b + \alpha c)uV + cV^2$$

zu verwandeln, in welcher der Coëfficient des ersten Gliedes

$$a + 2b\alpha + c\alpha^2$$

relativ prim zu der Determinante d ist.

Tragen wir, in der That, anstatt v den Werth

$$v = \alpha u + V$$

in

$$au^2 + 2buv + cv^2$$

ein, so erhalten wir:

$$au^2 + 2bu(\alpha u + V) + c(\alpha u + V)^2 =$$
$$(a + 2b\alpha + c\alpha^2)u^2 + 2(b + \alpha c)uV + cV^2,$$

wobei der Coëfficient $(a + 2b\alpha + c\alpha^2)$ des ersten Gliedes, nach Voraussetzung, relativ prim zur Determinante d ist.

Beispiel. Um

$$3u^2 + 2\,.\,21uv + 217v^2$$

in eine Form zu verwandeln, in welcher der Coëfficient des ersten Gliedes relativ prim zu ihrer Determinante 210 werde, bestimmen wir α so, dass

$$3 + 2\,.\,21\alpha + 217\alpha^2$$

zu 210 relativ prim werde. Wie wir oben gesehen haben genügt $\alpha = -2$ dieser Bedingung. Wir brauchen also nur

$$v + 2u = V$$

zu substituiren, also

$$v = V - 2u$$

in

$$3u^2 + 2\,.\,21uv + 217v^2$$

zu setzen. Wir erhalten dadurch

$$3u^2 + 2\,.\,21u(V-2u) + 217(V-2u)^2 =$$
$$787u^2 - 826uV + 217V^2$$

Auf diese Weise haben wir die Form

$$3u^2 + 2\,.\,21uv + 217v^2$$

allerdings in eine complicirtere

$$787u^2 - 826uV + 217V^2$$

verwandelt. Indess hat die letztere Form den Vorzug, dass der Coëfficient von u^2 relativ prim zur Determinante ist. Diese Eigenschaft wird uns zur Erleichterung der Bestimmung der linearen Theiler einer Form dienen, indem wir jetzt von jeder quadratischen Form voraussetzen können, dass der Coëfficient des ersten Gliedes relativ prim zu ihrer Determinante ist. Unter dieser Voraus-

setzung wollen wir folgende Lehrsätze in Bezug auf quadratische Formen beweisen.

63. *Lehrsatz.* *Ist in einer quadratischen Form*

$$au^2 + 2buv + cv^2$$

der Coëfficient a *des ersten Gliedes relativ prim zur Determinante*

$$b^2 - ac = d,$$

so kann man eine Zahl l *bestimmen, welche die Congruenz*

$$au^2 + 2buv + cv^2 \equiv al^2 + 2bl + c \pmod{d}$$

befriedigt.

Beweis. Ist a relativ prim zu d, so kann man die Congruenz

$$a(au^2 + 2buv + cv^2) \equiv a(al^2 + 2bl + c) \pmod{d}$$

durch a dividiren, so dass jede Zahl, welche diese Congruenz befriedigt, auch unsere gesuchte Congruenz

$$au^2 + 2buv + cv^2 \equiv al^2 + 2bl + c \pmod{d}$$

befriedigen muss. Die zu Hülfe genommene Congruenz

$$a(au^2 + 2buv + cv^2) \equiv a(al^2 + 2bl + c) \pmod{d}$$

kann man aber so schreiben:

$$(au + bv)^2 - (b^2 - ac)v^2 \equiv (al + b)^2 - (b^2 - ac) \pmod{d}$$

und diese geht, mit Berücksichtigung von

$$b^2 - ac = d,$$

in die Congruenz

$$(au + bv)^2 \equiv (al + b)^2 \pmod{d}$$

über, welche befriedigt wird, wenn

$$al + b \equiv au + bv \pmod{d}$$

ist. Die letzte Congruenz ersten Grades in Bezug auf l hat aber immer eine Lösung, weil der Coëfficient a von l relativ prim zum Modul d ist. Dadurch ist der Lehrsatz bewiesen.

Auf Grund dieses Lehrsatzes schliessen wir, dass wenn für die verschiedenen Werthe von l die zugehörigen Werthe von $al^2 + 2bl + c$ nach Modul d den Zahlen

$$r_1, \quad r_2, \quad \ldots, \quad r_n$$

congruent sind, so sind denselben Zahlen auch die verschiedenen Werthe von $au^2 + 2buv + cv^2$ congruent. Dieses heisst doch aber so viel, als: jede durch diese quadratische Form darstellbare Zahl muss durch eine der linearen Formen

$$dm + r_1, \quad dm + r_2, \quad \ldots, \quad dm + r_n$$

darstellbar sein, wobei m eine beliebige Zahl ist.

Was nun die Zahlen $r_1, r_2, \ldots, r_n$ betrifft, denen alle möglichen Werthe von $al^2 + 2bl + c$ nach Modul d congruent sein sollen, so kann man dieselben dadurch finden, dass man diejenigen Zahlen aufsucht, welche diesem Ausdruck nach d congruent sind, wenn man l die Werthe

$$l = 0, 1, 2, \ldots, d-1$$

ertheilt. Weil alle übrigen Werthe von $al^2 + 2bl + c$ den diesen Werthen von l entsprechenden congruent sein werden.

Somit werden wir für die Darstellung aller durch

$$au^2 + 2buv + cv^2$$

definirten Zahlen die linearen Formen

$$dm + r_1, \quad dm + r_2, \quad \ldots, \quad dm + r_n$$

erhalten.

Jede dieser Formen kann aber in vier verschiedene zerlegt werden, je nachdem m eine von den Gestalten

$$4z, \quad 4z + 1, \quad 4z + 2, \quad 4z + 3$$

hat. So ergeben sich aus der ersten $dm + r_1$ der obigen Formen folgende vier:

$$4dz + r_1, \quad 4dz + d + r_1, \quad 4dz + 2d + r_1, \quad 4dz + 3d + r_1.$$

Wir wollen nun zusehen, welche von diesen Formen wegzulassen sind, wenn wir uns auf die ungeraden Werthe von

$$au^2 + 2buv + cv^2$$

beschränken. Wir beginnen mit einem ungeraden d.



Bei ungeradem d werden unter den vier Zahlen

$$r_1, \quad d + r_1, \quad 2d + r_1, \quad 3d + r_1$$

zwei gerade und zwei ungerade sein (vgl. Lehrsatz 10). Indem wir uns also auf die ungeraden Werthe von

$$au^2 + 2buv + cv^2$$

beschränken, haben wir unter den vier Formen

$$4dz + r_1, \quad 4dz + d + r_1, \quad 4dz + 2d + r_1, \quad 4dz + 3d + r$$

solche zwei wegzulassen, in welchen die z nicht enthaltenden Glieder gerade Zahlen sind. Es bleiben uns dann für die ungeraden Werthe der quadratischen Form zwei lineare Formen übrig, von denen die eine Zahlen von der Gestalt $4m+1$, die andere Zahlen von der Gestalt $4m+3$ liefern wird. (Vgl. § 44).

Von diesen zwei linearen Formen werden wir dann *eine* oder *beide* beibehalten, jenachdem die quadratische Form

$$au^2 + 2buv + cv^2$$

lauter Zahlen von der Gestalt $4m+1$ oder lauter $4m+3$, oder beiderlei zugleich liefert. Dieses erfahren wir aber durch folgende Ueberlegung.

Für u und v sind vier Annahmen möglich, nämlich:

$u = 2s$	$u = 2s + 1$	$u = 2s + 1$	$u = 2s$
$v = 2t$	$v = 2t$	$v = 2t + 1$	$v = 2t + 1$.

Tragen wir diese Werthepaare in die quadratische Form

$$au^2 + 2buv + cv^2$$

ein, so erhalten wir die zugehörigen Resultate in vier folgenden Gestalten:

$$4N, \quad 4N_1 + a, \quad 4N_2 + a + 2b + c, \quad 4N_3 + c,$$

indem wir durch

$$4N, \quad 4N_1, \quad 4N_2, \quad 4N_3$$

jeweils die Gesammtheit aller Glieder bezeichnen, welche den Factor 4 besitzen.

Daraus ersehen wir, dass wenn keine der Zahlen

$$a, \quad c, \quad a + 2b + c$$

die Gestalt $4m + 1$, oder die Gestalt $4m + 3$ besitzt, auch die Form

$$au^2 + 2buv + cv^2$$

nicht Zahlen von der entsprechenden Gestalt liefern kann.

Wenden wir uns nun zu dem Falle eines geraden d.

Ist d eine gerade Zahl, so werden alle vier Zahlen

$$r_1, \quad d + r_1, \quad 2d + r_1, \quad 3d + r_1,$$

gleichzeitig, entweder gerade, oder ungerade sein. Im *ersteren* Falle wird die quadratische Form

$$au^2 + 2buv + cv^2$$

überhaupt keine ungeraden Zahlen darstellen können. Im *anderen* Falle werden wir je nach dem Werthe der Zahlen

$$r_1, \quad d + r_1, \quad 2d + r_1, \quad 3d + r_1$$

erfahren, welche von den vier Gestalten

$$8m + 1, \quad 8m + 3, \quad 8m + 5, \quad 8m + 7$$

die Zahlen

$$4dz + r_1, \quad 4dz + d + r_1, \quad 4dz + 2d + r_1, \quad 4dz + 3d + r_1$$

annehmen. Darnach erfahren wir dann auch, welche unter diesen wegzulassen sind, sobald wir feststellen welche von den viererlei Zahlen

$$8m + 1, \quad 8m + 3, \quad 8m + 5, \quad 8m + 7$$

aus der quadratischen Form

$$au^2 + 2buv + cv^2$$

erhalten werden können.

Zu diesem Ende überlegen wir, dass wenn man die vier Annahmen über u und v

$$\begin{array}{l|l|l|l} u = 4s & u = 4s & u = 4s + 2 & u = 4s + 2 \\ v = 4t & v = 4t + 2 & v = 4t + 2 & v = 4t \end{array},$$

welche für

$$au^2 + 2buv + cv^2$$

nur gerade Zahlen liefern, ausschliesst, nur noch folgende fünf Annahmen über u, v übrig bleiben:

$u = 2s+1$	$u = 2s+1$	$u = 2s+1$	$u = 4s+2$	$u = 4s$
$v = 2t+1$	$v = 4t$	$v = 2t+2$	$v = 2t+1$	$v = 2t+1.$

Indem wir diese Werthe in

$$au^2 + 2buv + cv^2$$

eintragen, erhalten wir die entsprechenden Resultate in der Gestalt:

$$8N + a + 2b + c, \quad 8N_1 + a, \quad 8N_2 + a + 4b + 4c,$$
$$8N_3 + 4a + 4b + c, \quad 8N_4 + c,$$

wenn wir mit

$$8N, \quad 8N_1, \quad 8N_2, \quad 8N_3, \quad 8N_4$$

jeweils die Gesammtheit aller Glieder bezeichnen, die den Factor 8 besitzen. Zu solchen Gliedern gehören offenbar auch

$$4(s^2 + s), \quad 4(t^2 + t),$$

welche, wie man leicht sieht, durch 8 theilbar sind.

Daraus folgt, dass die durch die quadratische Form

$$au^2 + 2buv + cv^2$$

definirte Zahl nur dann eine der Gestalten

$$8m + 1, \quad 8m + 3, \quad 8m + 5, \quad 8m + 7$$

annehmen kann, wenn unter den Zahlen

$$a, \; c, \quad a + 2b + c, \quad 4a + 4b + c, \quad a + 4b + 4c$$

eine von jener Gestalt sich befindet. Dadurch wird dann zugleich bestimmt, welche von den vier linearen Formen

$$4dz + r_1, \; 4dz + d + r_1, \; 4dz + 2d + r_1, \; 4dz + 3d + r_1$$

die ungeraden Werthe von

$$au^2 + 2buv + cv^2$$

darstellen können, und welche dagegen ausgeschlossen werden müssen.

Wir wollen dieses durch ein Beispiel erläutern.

Beispiel. Wir haben oben gesehen, dass die ungeraden Theiler der Form $x^2 + 26y^2$ nur durch die vier quadratischen Formen

$u^2 + 26v^2$, $2u^2 + 13v^2$, $3u^2 + 2uv + 9v^2$, $5u^2 + 4uv + 6v^2$

dargestellt werden können.

Um die linearen Formen der Theiler der ersten von den vier quadratischen Formen, nämlich $u^2 + 26v^2$ zu bestimmen, bemerken wir zunächst, dass in der letzteren der Coëfficient von u^2 keinen gemeinsamen Theiler mit der Determinante derselben besitzt. Man kann daher den Lehrsatz 63 anwenden, wonach man schliessen kann, dass alle Werthe von

$$u^2 + 26v^2$$

nach Modul 26 denselben Zahlen congruent sind, wie die Werthe von

$$l^2 + 26,$$

welche $l = 0, 1, 2, \ldots, 25$ entsprechen. Die kleinsten Zahlen, welche nach Modul 26 congruent sind

$$0^2 + 26, \quad 1^2 + 26, \quad 2^2 + 26, \quad \ldots \quad 25^2 + 26,$$

findet man, wenn man die Reste nimmt, welche nach Division dieser Zahlen durch 26 verbleiben. Wir finden so dieselben:

$$0, 1, 4, 9, 16, 25, 10, 23, 12, 3, 22, 17, 14, 13.$$

Folglich müssen alle möglichen Werthe von $u^2 + 26v^2$, indem sie diesen Zahlen congruent sind, in folgenden Formen darstellbar sein:

$$26m + 0,\ 26m + 1,\ 26m + 4,\ 26m + 9,\ 26m + 16,$$
$$26m + 25,\ 26m + 10,\ 26m + 23,\ 26m + 12,\ 26m + 3,$$
$$26m + 22,\ 26m + 17,\ 26m + 14,\ 26m + 13.$$

Unter diesen sind nur

$$26m + 1,\ 26m + 9,\ 26m + 25,\ 26m + 23,\ 26m + 3,\ 26m + 17$$

ungerade und relativ prim zu 26. Nur diese behalten wir daher bei.

Indem wir nun

$$m = 4z,\ \ 4z + 1,\ \ 4z + 2,\ \ 4z + 3$$

setzen, erhalten wir:



$$\begin{array}{llll}
104z + 1, & 104z + 27, & 104z + 53, & 104z + 79, \\
104z + 9, & 104z + 35, & 104z + 61, & 104z + 87, \\
104z + 25, & 104z + 51, & 104z + 77, & 104z + 103, \\
104z + 23, & 104z + 49, & 104z + 75, & 104z + 101, \\
104z + 3, & 104z + 29, & 104z + 55, & 104z + 81, \\
104z + 17, & 104z + 43, & 104z + 69, & 104z + 95.
\end{array}$$

Um dann zu entscheiden, welche von diesen 24 Formen beizubehalten und welche wegzulassen sind, haben wir noch die Frage zu beantworten: welche von den vier Gestalten

$$8m + 1, \quad 8m + 3, \quad 8m + 5, \quad 8m + 7$$

besitzen die durch $u^2 + 26v^2$ darstellbaren Zahlen.

Wir haben gesehen, dass für die allgemeine Form

$$au^2 + 2buv + cv^2$$

über diese Frage immer die Gestalt der Zahlen

$$a, \; c, \quad a + 2b + c, \quad 4a + 4b + c, \quad a + 4b + 4c$$

entscheidet. Für unseren speciellen Fall $u^2 + 26v^2$ heissen nun diese Zahlen

$$1, \quad 26, \quad 1 + 26, \quad 4 + 26, \quad 1 + 4 \,.\, 26.$$

Unter diesen findet sich keine von der Gestalt

$$8m + 5, \quad \text{oder} \quad 8m + 7.$$

folglich müssen wir von den obengefundenen 24 Formen diejenigen weglassen, welche Zahlen von dieser Gestalt ergeben. Da nun

53, 61, 77, 29, 101, 69 die Gestalt $8m + 5$
und 79, 87, 103, 55, 23, 95 die Gestalt $8m + 7$

besitzen, so haben wir die 12 Formen

$$\begin{array}{llll}
104z + 53, & 104z + 61, & 104z + 77, & 104z + 29, \\
104z + 101, & 104z + 69, & 104z + 79, & 104z + 87, \\
104z + 103, & 104z + 55, & 104z + 23, & 104z + 95
\end{array}$$

wegzulassen und behalten somit nur die 12 Formen:

$$\begin{array}{llll}
104z + 1, & 104z + 27, & 104z + 9, & 104z + 35, \\
104z + 25, & 104z + 51, & 104z + 49, & 104z + 75, \\
104z + 3, & 104z + 81, & 104 \;\; + 17, & 104 \;\; + 43.
\end{array}$$

Indem wir uns nun zur Bestimmung der linearen Formen derjenigen Zahlen wenden, welche durch die zweite der obigen vier quadratischen Formen, nämlich $2u^2 + 13v^2$ darstellbar sind, sehen wir zunächst, dass Lehrsatz 63 hier nicht direct anwendbar ist, weil 2, der Coëfficient von u^2, nicht relativ prim zur Determinante -26 ist. Wir müssen daher zuerst diese Form, nach der obenangegebenen Methode, transformiren. Da nun 2 der grösste gemeinsame Theiler von 2 und 26 ist, so suchen wir eine Zahl α, für welche

$$\frac{2\alpha + 0}{2} = \alpha$$

relativ prim zu 26 werde. Dieser Bedingung genügt $\alpha = 1$. Um $2u^2 + 13v^2$ zu unserem Zwecke zu transformiren, brauchen wir also nur darin

$$v = u + V$$

zu setzen, wodurch unsere Form in

$$15u^2 + 26uV + 13V^2$$

verwandelt wird. In dieser Form ist der Coëfficient von u^2 relativ prim zur Determinante -26 und alle ihre Werthe sind, nach Lehrsatz 63, denjenigen Zahlen nach Modul 26 congruent, welche als Reste bei der Division von

$$15 \,.\, 0^2 + 26 \,.\, 0 + 13, \quad 15 \,.\, 1^2 + 26 \,.\, 1 + 13,$$
$$15 \,.\, 2^2 + 26 \,.\, 2 + 13, \quad \ldots, \quad 15 \,.\, 25^2 + 26 \,.\, 25 + 13$$

durch 26 verbleiben. Diese Reste sind:

13, 28, 21, 18, 19, 24, 7, 20, 11, 10, 5, 8, 15, 0

und diesen Zahlen müssen also alle Werthe von

$$15u^2 + 26uV + 13V^2$$

nach Modul 26 congruent sein, d. h. sie können nur unter den Formen

$26m + 13$, $26m + 28$, $26m + 21$, $26m + 18$, $26m + 19$,
$26m + 24$, $26m + 7$, $26m + 20$, $26m + 11$, $26m + 10$,
$26m + 5$, $26m + 8$, $26m + 15$, $26m + 0$

enthalten sein. Unter diesen 14 Formen liefern aber nur folgende 6:



$$26m + 21, \quad 26m + 19, \quad 26m + 7,$$
$$26m + 11, \quad 26m + 5, \quad 26m + 15$$

ungerade Zahlen, welche relativ prim zu 26 sind. Nur diese 6 behalten wir daher bei und, indem wir für m die Werthe

$$m = 4z, \quad 4z + 1, \quad 4z + 2, \quad 4z + 3$$

setzen, erhalten wir aus den 6 genannten Formen folgende 24:

$$\begin{array}{llll} 104z + 21, & 104z + 47, & 104z + 73, & 104z + 99, \\ 104z + 19, & 104z + 45, & 104z + 71, & 104z + 97, \\ 104z + 7, & 104z + 33, & 104z + 59, & 104z + 85, \\ 104z + 11, & 104z + 37, & 104z + 63, & 104z + 89, \\ 104z + 5, & 104z + 31, & 104z + 57, & 104z + 83, \\ 104z + 15, & 104z + 41, & 104z + 67, & 104z + 93. \end{array}$$

Es kann aber keine durch

$$15u^2 + 26uV + 13V^2$$

darstellbare Zahl die Gestalt

$$8m + 1, \quad \text{oder} \quad 8m + 3$$

haben, da keine der Zahlen

$$15, \; 13, \quad 15 + 26 + 13, \quad 4 \,.\, 15 + 2 \,.\, 26 + 13,$$
$$15 + 2 \,.\, 26 + 4 \,.\, 13$$

die Gestalt

$$8m + 1, \quad \text{oder} \quad 8m + 3$$

haben kann.

Es bleiben also für die Darstellung aller durch die quadratische Form

$$15u^2 + 26uV + 13V^2$$

definirten Zahlen, welche obendrein noch ungerade und relativ prim zur Determinante sind, nur die 12 lineare Formen

$$\begin{array}{llll} 104z + 21, & 104z + 47, & 104z + 45, & 104z + 71, \\ 104z + 7, & 104z + 85, & 104z + 37, & 104z + 63, \\ 104z + 5, & 104z + 31, & 104z + 15, & 104z + 93. \end{array}$$

Von den vier oben angeführten quadratischen Formen

$$u^2 + 26v^2, \quad 2u^2 + 13v^2;$$
$$3u^2 + 2uv + 9v^2, \quad 5u^2 + 4uv + 6v^2,$$

durch welche die Theiler von $x^2 + 26y^2$ dargestellt werden sollen, haben wir bis jetzt nur die ersten zwei

$$u^2 + 26v^2, \quad 2u^2 + 13v^2$$

behandelt. Um nun *alle* linearen Theiler von $x^2 + 26y^2$ zu finden, müssen wir noch die linearen Formen für die Zahlen aufsuchen, welche durch die zwei quadratischen Formen

$$3u^2 + 2uv + 9v^2, \quad 5u^2 + 4uv + 6v^2$$

darstellbar sind.

Man findet indess, dass sich dadurch keine neuen linearen Formen ergeben, dass vielmehr

die für $3u^2 + 2uv + 9v^2$ mit denen für $u^2 + 26v^2$
und die für $5u^2 + 4uv + 6v^2$ mit denen für $2u^2 + 13v^2$

übereinstimmen, die wir bereits gefunden haben.

Resummiren wir nun die ganze Untersuchung, so finden wir alle ungeraden Theiler von

$$x^2 + 26y^2,$$

welche relativ prim zu 26 sind, durch folgende 24 lineare Formen

$$\begin{array}{llll}
104z + 1, & 104z + 3, & 104z + 5, & 104z + 7, \\
104z + 9, & 104z + 15, & 104z + 17, & 104z + 21, \\
104z + 25, & 104z + 27, & 104z + 31, & 104z + 35, \\
104z + 37, & 104z + 43, & 104z + 45, & 104z + 47, \\
104z + 49, & 104z + 51, & 104z + 63, & 104z + 71, \\
104z + 75, & 104z + 81, & 104z + 85, & 104z + 93
\end{array}$$

bestimmt.

So kann man mit Hülfe quadratischer Formen die linearen Theiler von

$$x^2 \pm Dy^2$$

in allen Fällen bestimmen, gleichviel, ob D eine Primzahl oder eine zusammengesetzte Zahl ist.

Um bei dieser Bestimmung überflüssiges Rechnen zu ersparen, wollen wir jetzt ein Mittel angeben, durch welches man erkennen kann, ob zwei quadratische Formen, welche die Theiler von

$$x^2 \pm Dy^2$$

darstellen, auf gleiche linearen Formen führen, wie dieses in dem obigen Beispiele mit

$$u^2 + 26v^2 \text{ und } 3u^2 + 2uv + 9v^2,$$
$$2u^2 + 13v^2 \text{ und } 5u^2 + 4uv + 6v^2$$

der Fall war.

Zu dem Ende werden wir folgenden Lehrsatz beweisen.

64. *Lehrsatz. Sind*

$$au^2 + 2buv + cv^2, \; a_1 U^2 + 2b_1 UV + c_1 V^2$$

zwei quadratische Formen der Theiler von

$$x^2 - dy^2$$

und sind a, a_1 *relativ prim zu* d, *während für irgend eine Zahl* l

$$a_1 \equiv al^2 + 2bl + c \pmod{d}$$

ist, so kann man immer eine Zahl x *finden, welche die Congruenz*

$$a_1 x^2 + 2b_1 x + c_1 \equiv a\alpha^2 + 2b\alpha + c \pmod{d}$$

befriedigt.

Beweis. Wenn a und a_1 relativ prim zu d sind, so darf man eine Congruenz von der Gestalt

$$a^2 a_1 (a_1 x^2 + 2b_1 x + c_1) \equiv a^2 a_1 (a\alpha^2 + 2b\alpha + c) \pmod{d}$$

jedenfalls durch $a^2 a_1$ dividiren, so dass wenn die Möglichkeit dieser Congruenz bewiesen wäre, auch die zu beweisende Congruenz

$$a_1 x^2 + 2b_1 x + c_1 \equiv a\alpha^2 + 2b\alpha + c \pmod{d}$$

bestehen würde.

Man kann aber die erstere Congruenz auch so schreiben:

$$(aa_1x+ab_1)^2-a^2(b_1^2-a_1c_1) \equiv aa_1(a\alpha+b)^2-aa_1(b^2-ac) \pmod{d},$$

wobei sowohl

$$b_1^2-a_1c_1 = d, \quad \text{als auch} \quad b^2-ac = d$$

ist, weil nach Voraussetzung beide quadratische Formen

$$a_1 U^2 + 2b_1 UV + c_1 V^2, \quad au^2 + 2buv + cv^2$$

Theiler von x^2-dy^2 darstellen. (Vgl. Lehrsatz 59). Es verwandelt sich infolgedessen die letzte Congruenz in folgende:

$$(aa_1 x + ab_1)^2 \equiv aa_1(a\alpha + b)^2 \pmod{d}.$$

Diese Congruenz wird aber befriedigt, wenn

$$aa_1 x + ab_1 \equiv (a\alpha + b)(al + b) \pmod{d}$$

gesetzt wird.

Um sich davon zu überzeugen, braucht man nur zu bemerken, dass für diesen Werth von

$$aa_1x + ab_1$$

die obige Congruenz in

$$(a\alpha + b)^2(al + b)^2 \equiv aa_1(a\alpha + b)^2 \pmod{d}$$

übergeht. Da aber nach Voraussetzung

$$a_1 \equiv al^2 + 2bl + c \pmod{d}$$

war, woraus

$$aa_1 \equiv a(al^2 + 2bl + c) \pmod{d},$$

also auch

$$aa_1 \equiv (al + b)^2-(b^2-ac) \pmod{d}$$

folgt, so ergiebt sich daraus, auf Grund von

$$b^2-ac = d,$$

die Congruenz

$$(al + b)^2 \equiv aa_1 \pmod{d}.$$

Um also die Congruenz

$$a_1x^2 + 2b_1x + c_1 \equiv a\alpha^2 + 2b\alpha + c \pmod{d}$$

zu befriedigen, braucht man nur x so zu bestimmen, dass die Congruenz ersten Grades

$$aa_1x + ab_1 \equiv (a\alpha + b)(al + b) \pmod{d}$$

befriedigt werde. Dieses ist aber offenbar immer möglich,

weil nach Voraussetzung der Coëfficient aa_1 von x relativ prim zum Modul d war.

Somit ist der Lehrsatz bewiesen; und aus diesem, in Verbindung mit Lehrsatz 63, ergiebt sich folgender

Zusatz. Wenn a_1 nach Modul d irgend einem Werthe von $al^2 + 2bl + c$ congruent ist, so sind die durch die quadratischen Formen

$$au^2 + 2buv + cv^2, \quad a_1 U^2 + 2b_1 UV + c_1 V^2$$

definirten Zahlen ein und denselben Zahlen nach Modul d congruent; es bestehen daher dieselben linearen Formen $md + r$ für die eine quadratische Form, wie für die andere.

Was nun die Formen $4md + r$ betrifft, so haben wir oben bereits eine Methode kennen gelernt, wie man dieselben aus den Formen $md + r$ herleiten kann. Unmittelbar aus jener Methode ist zu ersehen, dass die Formen $4md + r$ für die beiden quadratischen Formen

$$au^2 + 2buv + cv^2, \quad a_1 U^2 + 2b_1 UV + c_1 V^2$$

verschieden, oder gleich sein werden, je nach der Gestalt der Zahlen

$$a, \quad c, \quad a + 2b + c,$$
$$a_1, \quad c_1, \quad a_1 + 2b_1 + c_1,$$

wenn d ungerade ist und je nach der Gestalt der Zahlen

$$a, \quad c, \quad a + 2b + c, \quad 4a + 4b + c, \quad a + 4b + 4c,$$
$$a_1, \quad c_1, \quad a_1 + 2b_1 + c_1, \quad 4a_1 + 4b_1 + c_1, \quad a_1 + 4b_1 + 4c_1,$$

wenn d gerade ist.

Hiermit schliessen wir die Theorie der Theiler einer quadratischen Form

$$x^2 \pm dy^2.$$

Am Schlusse dieses Buches sind Tabellen der linearen Theiler solcher Formen für alle d zusammengestellt, welche durch kein Quadrat theilbar sind, von $d = 1$, bis $d = 101$. Diese Tabellen gewähren eine sehr wichtige Anwendung, wie wir dieses im nächsten Kapitel ersehen werden.



Kapitel VIII.

Anwendung der Theorie der Congruenzen auf die Zerlegung von Zahlen in Primzahlfactoren.

---

§ 48. Zerlegung der Zahlen in Primzahlfactoren durch die Bestimmung der Gestalt der Theiler.

Zum Schlusse der Theorie der Congruenzen wollen wir zeigen, wie man mit Hülfe derselben die Zerlegung der Zahlen in Primzahlfactoren bedeutend vereinfachen kann.

Um eine Zahl A in ihre Primzahlfactoren zu zerlegen, muss man, bekanntlich, zunächst die kleinste Primzahl aufsuchen, durch welche A theilbar ist; heisst diese Primzahl etwa α, so theilt man erst A durch α und sucht dann die kleinste Primzahl, durch welche $\frac{A}{\alpha}$ theilbar ist; heisst eine solche Primzahl β, so sucht man dann die kleinste Primzahl, welche $\frac{A}{\alpha\beta}$ theilt und setzt diesen Process so lange fort, bis man zu einem Quotienten gelangt, welcher durch keine Primzahl, die kleiner, als seine Quadratwurzel ist, ohne Rest getheilt werden kann. Dieser Quotient ist dann selbst eine Primzahl und das Product dieses Quotienten mit $\alpha\,\beta\,\ldots.$ [unter welchen Factoren auch mehrere einander gleich sein können] stellt dann die gesuchte Zerlegung der Zahl A in Primzahlfactoren dar. Somit führt der Process der Zerlegung einer Zahl in Primzahlfactoren auf die Untersuchung, ob diese gegebene

Zahl Theiler überhaupt hat, oder nicht, und, falls sie solche hat, welcher von den Theilern der kleinste ist. Diese Untersuchung macht aber, wenn die Zahl bedeutend gross ist ungeheure Schwierigkeiten. Um den kleinsten Theiler einer Zahl N mit den Hülfsmitteln der Arithmetik aufzusuchen, bleibt nichts anderes übrig, als unter allen Primzahlen, welche kleiner als $\sqrt{N}$ sind, solche Theiler dadurch zu suchen, dass man einfach versucht die Division wirklich auszuführen. Wenn aber N gross genug ist, so werden viele solcher Primzahlen vorhanden sein und man wird nicht selten gezwungen sein eine bedeutende Anzahl derselben auszuprobieren, bis man auf eine Primzahl kommen wird, welche Theiler von N ist. Noch viel grösseren Schwierigkeiten begegnen wir, falls N eine Primzahl ist; in diesem Falle muss man die Theilbarkeit von N in Bezug auf *alle* Primzahlen, welche kleiner als $\sqrt{N}$ sind, untersuchen. So würden wir, wenn wir auf die Principien der Arithmetik allein angewiesen wären, bei der Untersuchung der Bestandtheile irgend einer Zahl, welche 1000000 übertrifft, nicht selten gezwungen sein mehr als 160 Divisionen auszuführen, weil wir die Anzahl der Primzahlen, welche kleiner als $\sqrt{1000000} = 1000$ sind, 168 finden.

Auf Grund der Theorie der Congruenzen werden diese Untersuchungen bedeutend erleichtert, indem sie uns in den Stand setzt aus der Gestalt einer gegebenen Zahl direct über die nothwendige Gestalt aller möglichen Theiler derselben Schlüsse zu ziehen, so dass wir dann nur noch alle Zahlen von bestimmter Form zu untersuchen haben.

---

§ 49. **Bestimmung der Theiler einer Zahl von der Form $a^m \pm 1$.**

Wir beginnen mit einem besonders bemerkenswerthen speciellen Fall und indem wir mit Hülfe der im Kapitel V bewiesenen Lehrsätze hier folgende Lehrsätze beweisen, wollen wir zeigen, wie man die Formen aller Theiler einer Zahl bestimmen kann, wenn diese Zahl die Form $a^m \pm 1$ hat.

65. *Lehrsatz.* *Ist p eine ungerade Zahl und ein Theiler von $a^m - 1$, so kann p durch die Form*

$$\omega z + 1$$

dargestellt werden, wobei ω ein Theiler von m (u. zw. der grösste gemeinsame Theiler von m und $p-1$, also $\omega = 1$, wenn m und $p-1$ relativ prim), *während z relativ prim zu $\frac{m}{\omega}$ ist; und p muss zugleich auch Theiler von $a^\omega - 1$ sein.*

Beweis. Ist ω der grösste gemeinsame Theiler von $p-1$ und m, so sind $\frac{p-1}{\omega}$, $\frac{m}{\omega}$ ganze Zahlen und relativ prim zu einander. Bezeichnet man die erstere dieser beiden Zahlen mit z, so erhält man

$$\frac{p-1}{\omega} = z,$$

woraus sich

$$p = \omega z + 1$$

ergiebt.

Es bleibt uns nur noch übrig zu zeigen, dass p ein Theiler von $a^\omega - 1$ sein muss. Wir bemerken zu dem Ende, dass die Theilbarkeit von $a^m - 1$ durch p durch die Congruenz

$$a^m - 1 \equiv 0 \pmod{p}$$

ausgedrückt wird. Haben $p-1$ und m den grössten gemeinsamen Theiler ω, so folgt, nach Lehrsatz 35, aus der letzten Congruenz auch die Congruenz

$$a^\omega - 1 \equiv 0 \pmod{p},$$

d. h. die Theilbarkeit von $a^\omega - 1$ durch p, was zu beweisen war. Auch folgenden Lehrsatz kann man mit Hülfe des vorhergehenden leicht beweisen.

66. *Lehrsatz.* *Ist $2n + 1$ eine Primzahl, so müssen die ungeraden Primzahlen, welche Theiler von*

$$a^{2n+1}-1$$

sind, entweder die Form

$$2(2n+1)z+1$$

haben, oder Theiler von

$$a-1$$

sein; ausserdem müssen dieselben auch Theiler der quadratischen Form

$$x^2-ay^2$$

sein.

Beweis. Wenn p eine ungerade Zahl ist, so kann man dieselbe durch

$$2N+1$$

darstellen. Ist dann N durch $2n+1$ theilbar, so hat p die Form

$$p = 2(2n+1)z+1.$$

Ist dagegen N durch die Primzahl $2n+1$ nicht theilbar, so ist $2N$ relativ prim zu $2n+1$. Ist aber

$$p = 2N+1$$

ein Theiler von

$$a^{2n+1}-1,$$

während $2N$ relativ prim zu $2n+1$ ist, so muss p, nach vorhergehendem Lehrsatze, Theiler von

$$a-1$$

sein. Folglich muss p entweder die Form

$$p = 2(2n+1)z+1$$

haben, oder Theiler von $a-1$ sein.

Wir wollen nun noch beweisen, dass p ein Theiler der quadratischen Form

$$x^2-ay^2$$

sein muss.

Davon kann man sich leicht überzeugen. Es ist nach Voraussetzung p ein Theiler von

$$a^{2n+1}-1,$$

folglich auch ein Theiler von

$$a(a^{2n+1}-1) = (a^{n+1})^2-a.$$

Die rechte Seite dieser Gleichung hat aber, für $x = a^{n+1}$ und $y = 1$, die Form

$$x^2 - ay^2.$$

Indem wir noch bemerken, dass für $a = 2$ überhaupt keine Zahl Theiler von $a - 1$ sein kann, während, nach Lehrsatz 55 alle Theiler von $x^2 - ay^2$ in diesem Falle entweder die Form $8m + 1$, oder $8m - 1$ haben müssen, so ergiebt sich daraus, auf Grund des letzten Lehrsatzes, folgender

Zusatz. *Alle Primzahlfactoren von* $2^{2n+1} - 1$, *haben, wenn* $2n + 1$ *eine Primzahl ist, die Form* $2(2n + 1)z + 1$ *und zu gleicher Zeit müssen sie auch entweder die Form* $8m + 1$, *oder die Form* $8m - 1$ *haben.*

Indem wir in solcher Weise die nothwendige Form aller Theiler von

$$2^{2n+1} - 1$$

bestimmt haben, können wir in jedem gegebenen Falle diese Theiler entweder wirklich auffinden, oder den Beweis führen, dass solche überhaupt nicht vorhanden sind.

Auf diesem Wege hat *Euler* gefunden, dass

$$2^{31} - 1 = 2147483647$$

eine Primzahl ist und diese ist überhaupt die grösste Primzahl, welche wir bis jetzt [*)] kennen.

In ähnlicher Weise kann man auch jede andere Zahl von der Form $a^m - 1$ untersuchen.

Wir wenden uns jetzt zu den Zahlen von der Form $a^m + 1$ und beweisen folgenden Lehrsatz in Bezug auf die Theiler solcher Zahlen.

67. *Lehrsatz.* *Ist* p *eine ungerade Primzahl und Theiler von* $a^m + 1$, *so kann* p *durch die Form*

$$2\omega z + 1$$

dargestellt werden, wobei ω *ein Thei-*

[*) Seitdem der Verfasser dieses geschrieben hat (1849) sind auch weitere Beispiele gerechnet worden].

ler von m (u. zw. d. gr. gem. Th. von m und $p-1$, also $\omega = 1$, wenn m und $p-1$ rel. prim), *welcher zum Quotienten* $\frac{m}{\omega}$ *eine ungerade Zahl ergiebt, während* z *relativ prim zu* $\frac{m}{\omega}$ *ist; und* p *muss zugleich auch Theiler von* $a^\omega + 1$ *sein.*

Beweis. Die Theilbarkeit von $a^m + 1$ durch p wird durch die Congruenz

$$a^m + 1 \equiv 0 \pmod{p}$$

ausgedrückt, mit welcher, nach Lehrsatz 39, zugleich die Congruenz

$$a^\omega + 1 \equiv 0 \pmod{p}$$

bestehen muss, wenn ω der grösste gemeinschaftliche Theiler von m und $p-1$ ist, welcher zum Quotienten $\frac{p-1}{\omega}$ eine gerade Zahl ergeben muss, wenn p ungerade ist. Setzt man diesen Quotienten gleich $2z$, so findet man $\frac{p-1}{\omega} = 2z$, also:

$$p = 2\omega z + 1.$$

Man kann sich aber leicht überzeugen, dass z relativ prim zu $\frac{m}{\omega}$ und der Quotient $\frac{m}{\omega}$ ungerade ist. Indem nämlich ω den grössten gemeinsamen Theiler von m und $p-1$ ausmacht, müssen die Quotienten

$$\frac{p-1}{\omega}, \quad \frac{m}{\omega}$$

relativ prim zueinander sein. Da aber der erstere dieser Quotienten $2z$ ist, so kann derselbe nur dann relativ prim zu $\frac{m}{\omega}$ sein, wenn $\frac{m}{\omega}$ durch 2 nicht theilbar ist und zugleich $\frac{m}{\omega}$ mit z keinen Theiler gemein hat.

Da nun aus der obigen Congruenz $a^\omega + 1 \equiv 0 \pmod{p}$ direct hervorgeht, dass p Theiler von

$$a^\omega + 1$$

sein muss, so ist der Lehrsatz in allen Theilen bewiesen.

Folgender Lehrsatz ergiebt sich dann als specieller Fall des vorhergehenden.

68. *Lehrsatz. Die ungeraden Primzahlfactoren einer Zahl*

$$a^{2n+1} + 1$$

müssen, entweder die Form

$$2(2n + 1)z + 1$$

haben, oder Theiler von

$$a + 1$$

sein.

Beweis. Die ungerade Zahl p hat die Form

$$2N + 1.$$

Ist nun N durch $2n + 1$ theilbar, so hat p die Form

$$p = 2(2n + 1)z + 1.$$

Ist aber N durch die Primzahl $2n + 1$ nicht theilbar, so ist $2N$ relativ prim zu $2n + 1$ und die Theilbarkeit von $a^{2n+1} + 1$ durch $p = 2N + 1$ bedingt dann, nach dem vorhergehenden Lehrsatze, die Theilbarkeit von $a + 1$ durch p, was wir beweisen wollten.

69. *Lehrsatz. Alle ungeraden Theiler von*

$$2^{2^n} + 1$$

müssen die Form haben:

$$2^{n+1}. z + 1.$$

Beweis. Nach Lehrsatz 67 können die ungeraden Theiler von $2^{2^n} + 1$ durch $2 . \omega z + 1$ dargestellt werden, wobei ω ein Theiler von 2^n sein muss, der als Quotienten $\frac{2^n}{\omega}$ eine ungerade Zahl liefert. Dieser Bedingung kann in unserem Falle nur $\omega = 2^n$ befriedigen, folglich müssen alle ungeraden Theiler von $2^{2^n} + 1$ die Form

$$2 . 2^n z + 1 = 2^{n+1} . z + 1$$

haben, was zu beweisen war.

Auf Grund der letzten drei Lehrsätze kann man leicht die Theiler einer Zahl von der Gestalt $a^m + 1$ finden, oder sich überzeugen, dass diese Zahl überhaupt keine Theiler besitzt.

Beispiele. 1) Es sollen die Theiler von 65537 gefunden werden. Diese Zahl hat die Gestalt $2^{2^4}+1$; folglich müssen nach Lehrsatz 69 alle Theiler von 65537 die Form $32 . z + 1$ haben. Setzt man darin für z die Werthe

$$z = 1, 2, 3, 4, 5, 6, 7, 8,$$

so findet man, dass alle Zahlen, welche die vorgeschriebene Form haben und kleiner als $\sqrt{65537}$ sind, nur die ersten 7 von folgenden 8 Zahlen sein können:

$$33, 65, 97, 129, 161, 193, 225, 257.$$

Unter diesen sind nur 97 und 193 Primzahlen. Da nun diese beiden keine Theiler von 65537 sind, so schliessen wir daraus dass 65537 eine Primzahl ist.

2) Die Theiler von 4294967297 sollen gefunden werden. Diese Zahl hat die Form $2^{2^5} + 1$; ihre Theiler müssen daher nach demselben Lehrsatze 69, wie im vorigen Beisp. die Form $64z + 1$ haben.

Ertheilt man hierbei z die Werthe

$$z = 1, 2, 3, \ldots, 1024,$$

so findet man alle Zahlen, welche die vorgeschriebene Form haben und kleiner als $\sqrt{4294967297}$ sind. Darunter sind

$$193, 257, 449, 577, 641, \ldots$$

Primzahlen. Indem man durch die letzteren 4294967297 zu dividiren versucht, findet man, dass 641 wirklich ein Theiler ist.

Dieses Beispiel ist insofern von besonderem Interesse, als es die Behauptung *Fermat's: „jede Zahl von der Gestalt* $2^{2^n} + 1$ *sei eine Primzahl*“, widerlegt.

---

§ 50. **Bestimmung der Theiler von Zahlen auf Grund der Theorie der Theiler von $x^2 \pm ay^2$**

Wir haben gesehen, wie die Theorie der binomischen Congruenzen die Untersuchung der Theiler von Zahlen, welche die Gestalt $a^m \pm 1$ haben, erleichtert. Wir wollen

nunmehr zeigen, wie man für irgend eine Zahl A viele Formen

$$x^2 \pm ay^2$$

finden kann, in welchen a keine grosse Zahl wird und diese Formen sollen entweder die Zahl A selbst oder ein Vielfaches derselben darstellen. Die Theiler von A werden dann jedenfalls auch Theiler dieser Formen sein und somit wird man die Form dieser Theiler nach den im vorhergehenden Kapitel angegebenen Methoden bestimmen können; oder man wird die Theiler in den Tabellen für die Theiler von $x^2 \pm ay^2$ am Schlusse dieses Buches aufsuchen können, wenn a nicht 101 übertrifft.

Was für eine Zahl A auch sein mag, kann man immer A selbst, oder ein Vielfaches kA durch eine Form $x^2 \pm ay^2$ *darstellen.*

Nimmt man für x irgend eine beliebige Zahl und für y die grösste Zahl, deren Quadrat ein Theiler von $A-x^2$ ist und bezeichnet dann den Quotienten der Division von $A-x^2$ durch y^2 mit a, so erhält man

$$\frac{A-x^2}{y^2} = a, \quad \text{oder} \quad A = x^2 + ay^2.$$

In ähnlicher Weise kann man die Zahlen $2A$, $3A$, ... darstellen. Alle so erhaltenen Formen werden dazu dienen können, die Form der Theiler von A zu bestimmen. Unter ihnen werden diejenigen am bequemsten sein, in denen a eine möglichst kleine Zahl ist; weil, wie wir aus der Theorie der Theiler quadratischer Formen gesehen haben, die Formen der Theiler von $x^2 \pm ay^2$ umso einfacher sind, je kleiner die Zahl a ist. Wir müssen daher unter allen Formen $x^2 \pm ay^2$, welche A, oder kA darstellen, diejenigen wählen, bei denen a am kleinsten ist. Für manche Zahlen kann man solche Formen unmittelbar finden. So ist z. B. sofort zu ersehen, dass

$$10001 = 100^2 + 1; \quad 3 \,.\, 3337 = 100^2 + 11, \quad \text{u. dgl.}$$

Allgemein aber kann man auf Grund des folgenden Lehrsatzes immer solche Formen bilden.

70. *Lehrsatz.* *Sind in der Reihe*

$$d_0, \quad d_1, \quad d_2, \quad \ldots .$$

die d Zahlen, welche dadurch definirt sind, dass je drei aufeinanderfolgende

$$d_{n-1}, \quad d_n, \quad d_{n+1}$$

immer die Gleichung

$$\sqrt{A - d_{n+1}\, d_n} = d_n\, E\, \frac{\sqrt{A - d_n\, d_{n-1}} + \sqrt{A}}{d_n} - \sqrt{A - d_n\, d_{n-1}} \; (*)$$

befriedigen, während die ersten zwei die Werthe

$$d_0 = 1; \quad d_1 = A - (E\sqrt{A})^2$$

haben, so besitzt jede der Formen

$$x^2 - Dy^2$$

wobei D den Werth

$$D = (-1)^{\alpha+\beta+\gamma\cdots}\, d_\alpha\, d_\beta\, d_\gamma \ldots .$$

hat, die Eigenschaft die Zahl A, oder ein Vielfaches von A darzustellen.

Beweis. Bevor wir zum eigentlichen Beweise des Lehrsatzes schreiten, wollen wir zunächst beweisen, dass die Reihen

$$d_0, \quad d_1, \quad d_2, \quad \ldots .$$

$$\sqrt{A - d_1\, d_0}, \quad \sqrt{A - d_2\, d_1}, \quad \sqrt{A - d_3\, d_2}, \quad \ldots .$$

aus lauter ganzen Zahlen bestehen.

Nach der Voraussetzung waren

$$d_0 = 1, \quad d_1 = A - (E\sqrt{A})^2,$$

woraus zunächst folgt, dass

$$d_0, \quad d_1, \quad \sqrt{A - d_1, d_0}$$

ganze Zahlen sind. Sind diese aber ganze Zahlen, so können auch alle übrigen Glieder der Reihen

$$d_0, \quad d_1, \quad d_2, \quad d_3, \quad \ldots .$$

$$\sqrt{A - d_1\, d_0}, \quad \sqrt{A - d_2\, d_1}, \quad \sqrt{A - d_3\, d_2}, \quad \ldots .$$

(*) E soll hier dieselbe Bedeutung, wie in § 26 haben.

keine gebrochenen oder irrationalen Zahlen sein. Denn aus der Gleichung

$$\sqrt{A - d_{n+1} d_n} = d_n E \frac{\sqrt{A - d_n d_{n-1}} + \sqrt{A}}{d_n} - \sqrt{A - d_n d_{n-1}},$$

welche überhaupt die d definirt, folgt:

$$d_{n+1} = d_{n-1} + 2\sqrt{A - d_n d_{n-1}}\, E \frac{\sqrt{A - d_n d_{n-1}} + \sqrt{A}}{d_n} + \\ + d_n \left[E \frac{\sqrt{A - d_n d_{n-1}} + \sqrt{A}}{d_n}\right]^2.$$

Aus der letzten Gleichung ersieht man, dass d_{n+1} eine ganze Zahl sein muss, sobald

$$d_{n-1}, \quad d_n, \quad \sqrt{A - d_n d_{n-1}}$$

solche sind und aus der vorletzten Gleichung, dass unter denselben Voraussetzungen auch $\sqrt{A - d_{n+1} d_n}$ eine ganze Zahl ist. Nun wissen wir aber bereits, dass

$$d_0, \quad d_1, \quad \sqrt{A - d_1 d_0}$$

ganze Zahlen sind, folglich müssen auch

$$d_2, \quad \sqrt{A - d_2 d_1}$$

ganze Zahlen sein. Sind aber

$$d_1, \quad d_2, \quad \sqrt{A - d_2 d_1}$$

ganze Zahlen, so müssen es auch

$$d_3, \quad \sqrt{A - d_3 d_2}$$

sein, etc.

Indem wir nun zum Beweise des Lehrsatzes übergehen, bezeichnen wir die Ausdrücke

$$\sqrt{A - d_1 d_0}, \ \sqrt{A - d_2 d_1}, \ \ldots, \ \sqrt{A - d_{n-1} d_{n-2}}, \ \sqrt{A - d_n d_{n-1}}$$

respective mit $x_0, x_1, \ldots, x_{n-2}, x_{n-1}$, welche, wie wir gesehen haben, ganze Zahlen sein werden. Quadrirt man die Gleichungen

$$x_0 = \sqrt{A - d_1 d_0}, \quad x_1 = \sqrt{A - d_2 d_1}, \quad x_2 = \sqrt{A - d_3 d_2} \ \ldots \\ x_{n-2} = \sqrt{A - d_{n-1} d_{n-2}}, \quad x_{n-1} = \sqrt{A - d_n d_{n-1}},$$

so erhält man

$$x_0^2-A = -d_1 d_0; \quad x_1^2-A = -d_2 d_1; \quad x_2^2-A = -d_3 d_2,$$
$$\ldots . x_{n-2}^2-A = -d_{n-1} d_{n-2}, \quad x_{n-1}^2-A = -d_n d_{n-1},$$

welche man auch so schreiben kann:

$$\begin{aligned}
(x_0 + \sqrt{A})(x_0-\sqrt{A}) &= -d_1 d_0, \\
(x_1 + \sqrt{A})(x_1-\sqrt{A}) &= -d_2 d_1, \\
(x_2 + \sqrt{A})(x_2-\sqrt{A}) &= -d_3 d_2, \\
&\vdots \\
(x_{n-2} + \sqrt{A})(x_{n-2}-\sqrt{A}) &= -d_{n-1} d_{n-2}, \\
(x_{n-1} + \sqrt{A})(x_{n-1}-\sqrt{A}) &= -d_n d_{n-1}.
\end{aligned}$$

Multiplicirt man alle diese Gleichungen mit einander, so erhält man

$$(x_0+\sqrt{A})(x_1+\sqrt{A})(x_2+\sqrt{A})\ldots(x_{n-2}+\sqrt{A})(x_{n-1}+\sqrt{A}) \times$$
$$(x_0-\sqrt{A})(x_1-\sqrt{A})(x_2-\sqrt{A})\ldots(x_{n-2}-\sqrt{A})(x_{n-1}-\sqrt{A})$$
$$= (-1)^n d_0 d_1^2 d_2^2 \ldots d_{n-2}^2 d_{n-1}^2 d_n.$$

Indem man aber die Multiplication der Factoren

$$x_0 + \sqrt{A}, \quad x_1 + \sqrt{A}, \ \ldots, \ x_{n-1} + \sqrt{A}$$

unter einander, beziehungsweise die der Factoren

$$x_0 - \sqrt{A}, \quad x_1 - \sqrt{A}, \ \ldots, \ x_{n-1} - \sqrt{A}$$

unter einander ausführt, erhält man als Product eine Zahl von der Form

$$X_n + Y_n\sqrt{A} \text{ beziehungsweise } X_n - Y_n\sqrt{A},$$

wobei X_n und Y_n ganze Zahlen sind. In Folge dieser Bemerkung geht die obige Gleichung in folgende über:

$$(X_n + Y_n\sqrt{A})(X_n - Y_n\sqrt{A}) = (-1)^n d_0 d_1^2 d_2^2 \ldots d_{n-1}^2 d_n$$

Setzt man

$$d_1 d_2 d_3 \ldots d_{n-1} = Z_n$$

und bemerkt, dass $d_0 = 1$ ist, so erhält man

$$(X_n + Y_n\sqrt{A})(X_n - Y_n\sqrt{A}) = (-1)^n . Z_n^2 . d_n.$$

Eine solche Gleichung erhalten wir für jede ganze Zahl n.

Ertheilt man nun n die Werthe

$$n = \alpha, \quad n = \beta, \quad n = \gamma, \quad \ldots,$$

so erhält man:

$$(X_\alpha + Y_\alpha \sqrt{A})(X_\alpha - Y_\alpha \sqrt{A}) = (-1)^\alpha Z_\alpha^2 \cdot d_\alpha$$
$$(X_\beta + Y_\beta \sqrt{A})(X_\beta - Y_\beta \sqrt{A}) = (-1)^\beta Z_\beta^2 \cdot d_\beta$$
$$(X_\gamma + Y_\gamma \sqrt{A})(X_\gamma - Y_\gamma \sqrt{A}) = (-1)^\gamma Z_\gamma^2 \cdot d_\gamma$$
$$\cdots\cdots\cdots\cdots$$

Multiplicirt man alle diese Gleichungen mit einander und berücksichtigt, dass das Product aller Factoren

$$X_\alpha + Y_\alpha \sqrt{A}, \quad X_\beta + Y_\beta \sqrt{A}, \quad X_\gamma + Y_\gamma \sqrt{A}, \ \ldots$$

die Form $X + Y\sqrt{A}$ und das Product von

$$X_\alpha - Y_\alpha \sqrt{A}, \quad X_\beta - Y_\beta \sqrt{A}, \quad X_\gamma - Y_\gamma \sqrt{A}, \ \ldots$$

die Form $X - Y\sqrt{A}$ annimmt, wobei X, Y ganze Zahlen sind, so erhält man

$$(X + Y\sqrt{A})(X - Y\sqrt{A}) = (-1)^{\alpha+\beta+\gamma\ldots} Z_\alpha^2 Z_\beta^2 Z_\gamma^2 \ldots d_\alpha d_\beta d_\gamma \ldots,$$

oder auch

$$X^2 - A Y^2 = (-1)^{\alpha+\beta+\gamma+\cdots} d_\alpha d_\beta d_\gamma \ldots (Z_\alpha Z_\beta Z_\gamma \ldots)^2,$$

oder auch so geschrieben:

$$X^2 - (-1)^{\alpha+\beta+\gamma+\cdots} d_\alpha d_\beta d_\gamma \ldots (Z_\alpha Z_\beta Z_\gamma \ldots)^2 = Y^2 A.$$

Daraus ersieht man, dass die quadratische Form

$$x^2 - Dy^2$$

ein Vielfaches von A darstellt, sobald

$$D = (-1)^{\alpha+\beta+\gamma+\cdots} d_\alpha d_\beta d_\gamma \ldots,$$
$$x = X \text{ und } y = Z_\alpha Z_\beta Z_\gamma \ldots$$

bedeuten, was zu beweisen war.

Auf Grund dieses Lehrsatzes kann man viele Formen

$$x^2 \pm ay^2$$

finden, welche ein Vielfaches von A darstellen können, indem man die Zahlen

$$d_0, \quad d_1, \quad d_2, \ \ldots$$

bestimmt.

In diesen Formen wird a als ein Product aus irgend welchen von den Zahlen

$$d_0, \quad d_1, \quad d_2, \quad \ldots.$$

bestimmt und wir werden nur unter den Combinationen dieser Zahlen solche zu wählen suchen, deren Product ein vollständiges Quadrat, multiplicirt mit einer möglichst kleinen Zahl werde.

Indem wir ein solches Product zur Bestimmung von a wählen und unter den Factoren von a jedes vollständige Quadrat, auf Grund von § 46, weglassen, erhalten wir Formen

$$x^2 \pm ay^2$$

mit genügend kleinen Coëfficienten, welche, nach der obigen Auseinandersetzung, dazu dienen werden, die Theiler von A zu bestimmen.

Allerdings werden unter diesen Formen die Zahlen

$$d_1, \quad d_2, \quad d_3, \quad \ldots.$$

nicht enthalten sein, obwohl sie auch Theiler von A sein können. Wir werden daher vor Allem A durch diese Zahlen zu dividiren versuchen, um uns zu überzeugen, ob sie nicht selbst Theiler von A seien.

Sollten auf diese Weise die gefundenen Formen nicht ausreichen, um alle Theiler zu finden, so könnten wir auf Grund des vorhergehenden Lehrsatzes noch Formen aufsuchen, welche Vielfache

$$2A, \quad 3A, \quad 4A, \quad \ldots.$$

darstellen und unter denselben solche herauswählen, welche für die Bestimmung aller Theiler von A am geeignetsten sind.

Beispiel. Es sollen alle Theiler von 8520191 gefunden werden.

Ohne uns bei der Aufsuchung solcher Formen, welche etwa *unmittelbar* für die Darstellung von 8520191 oder einem Vielfachen derselben gefunden werden könnten, länger aufzuhalten, wollen wir solche Formen mit Hülfe des vorhergehenden Lehrsatzes aufsuchen.

Zu diesem Zwecke müssen wir vor Allem die Zahlen

$$d_0, \quad d_1, \quad d_2, \quad \ldots.$$

aus den Gleichungen

$$d_0 = 1, \quad d_1 = 8520191 - (E\sqrt{8520191})^2,$$

$$\sqrt{8520191 - d_{n+1}\,d_n} = d_n\, E\frac{\sqrt{8520191 - d_n\,d_{n-1}} + \sqrt{8520191}}{d_n} - \sqrt{8520191 - d_n\,d_{n-1}}$$

berechnen.

Man erhält aus diesen Gleichungen folgende Werthe:

$d_0 = 1$,	$d_4 = 1313,$	$d_8 = 1169,$	$d_{12} = 593,$	$d_{16} = 1210,$
$d_1 = 5467,$	$d_5 = 2630,$	$d_9 = 4523,$	$d_{13} = 2854,$	....
$d_2 = 370,$	$d_6 = 3185,$	$d_{10} = 242,$	$d_{14} = 2965,$	....
$d_3 = 4319,$	$d_7 = 203,$	$d_{11} = 1855,$	$d_{15} = 371,$	....

Zerlegt man diese Zahlen in ihre Primzahlfactoren, was bei diesen kleinen Zahlen keine sehr grossen Schwierigkeiten bietet(*), so findet man:

$d_0 = 1$,	$d_4 = 13.101,$	$d_8 = 7.167,$	$d_{12} = 593$,	$d_{16} = 2.5.11^2$
$d_1 = 7.11.71,$	$d_5 = 2.5.263,$	$d_9 = 4523,$	$d_{13} = 2.1427,$	
$d_2 = 2.5.37,$	$d_6 = 5.7^2.13,$	$d_{10} = 2.11^2,$	$d_{14} = 5.593,$	
$d_3 = 7.617,$	$d_7 = 7.29,$	$d_{11} = 5.7.53,$	$d_{15} = 7.53$,	

Indem wir die Bestandtheile der Zahlen $d_0, d_1, \ldots, d_{10}$ näher betrachten, finden wir, dass

$$d_6, \quad d_{10}, \quad d_{16}, \quad d_{10}\,d_{16}, \quad d_6\,d_{10}\,d_{16}, \quad d_2\,d_{16}, \quad d_4\,d_6\,d_{10}\,d_{16}$$

sehr einfache Zahlen liefern, wenn die in ihnen enthaltenen vollständigen Quadrate vernachlässigt werden.

Wir nehmen daher, auf Grund des letzten Lehrsatzes, zur Bestimmung der Theiler unserer Zahl 8520191, quadratische Formen

$$x^2 - ay^2,$$

in welchen a folgende Werthe hat:

(*) Man kann sich dabei mit Vortheil der Tafeln von Vega bedienen, in welchen für alle Zahlen, welche kleiner als 102000 sind, die Zerlegung in Primzahlfactoren gegeben ist.

$$a = (-1)^6 d_6 = 5 . 7^2 . 13,$$
$$a = (-1)^{10} d_{10} = 2 . 11^2,$$
$$a = (-1)^{16} d_{16} = 2 . 5 . 11^2,$$
$$a = (-1)^{10+16} d_{10} d_{16} = 2^2 . 5 . 11^2,$$
$$a = (-1)^{6+10+16} d_6 d_{10} d_{16} = 2^2 . 5^2 . 7^2 . 11^2 . 13,$$
$$a = (-1)^{2+16} d_2 d_{16} = 2^2 . 5^2 . 11^2 . 37,$$
$$a = (-1)^{4+6+10+16} d_4 d_6 d_{10} d_{16} = 2^2 . 5^2 . 7^2 . 11^2 . 13^2 . 101.$$

Vernachlässigt man bei diesen Werthen von a die Factoren, welche vollständige Quadrate bilden, so erhält man für a die Werthe:

$$a = 5 . 13,\ \ 2,\ \ 2 . 5,\ \ 5,\ \ 13,\ \ 37,\ \ 101.$$

Daraus ersehen wir, dass die Theiler von 8520191 zugleicher Zeit Theiler der folgenden quadratischen Formen sein müssen:

$$x^2 - 5 . 13y^2,\ \ x^2 - 2y^2,\ \ x^2 - 2 . 5y^2,\ \ x^2 - 5y^2,$$
$$x^2 - 13y^2,\ \ x^2 - 37y^2,\ \ x^2 - 101y^2.$$

Auf Grund dieser Thatsache werden wir die Theiler von 8520191 auch wirklich aufsuchen können.

Aus unseren Tabellen der linearen Theiler ersehen wir, dass die quadratische Form $x^2 - 5 . 13y^2$ folgende Theiler besitzt

$260z +$ 1, 7, 9, 29, 33, 37, 47, 49, 51, 57, 61, 63, 67, 69, 73, 79, 81, 83, 93, 97, 101, 121, 123, 129, 131, 137, 139, 159, 163, 167, 177, 179, 181, 187, 191, 193, 197, 199, 203, 209, 211, 213, 223, 227, 231, 251, 253, 259.

Von diesen können nur diejenigen zugleich Theiler von $x^2 - 5y^2$ sein, welche nach Division durch 20 die Reste 1, 9, 11, 19 ergeben; weil wir für $x^2 - 5y^2$ die Theiler

$$20z + 1,\ 9,\ 11,\ 19$$

finden.

Lassen wir daher aus den vorhergehenden Formen diejenigen weg, welche nicht die Reste 1, 9, 11, 19 geben, so erhalten wir für die gleichzeitigen Theiler von

$$x^2 - 5 \, . \, 13y^2$$

und

$$x^2 - 5y^2$$

nur noch die linearen Formen

$$260z + 1, 9, 29, 49, 51, 61, 69, 79, 81, 101, 121, 129, 131, 139, 159, 179, 181, 191, 199, 209, 211, 231, 251, 259.$$

Aus diesen können aber nur diejenigen zugleich auch Theiler der quadratischen Form $x^2 - 2y^2$ sein, welche die Form

$$8z + 1, \quad \text{oder} \quad 8z + 7$$

haben, welche also bei Division durch 8 den Rest 1, oder 7 liefern.

Um aus den gefundenen linearen Formen der gemeinsamen Theiler von $x^2 - 5 \, . \, 13y^2$ und $x^2 - 5y^2$ diejenigen herauszufinden, welche Zahlen von der Form $8z + 1$, oder $8z + 7$ ergeben, transformiren wir dieselben so, dass der Coëfficient der Veränderlichen z ein Vielfaches von 8 werde. Zu diesem Zwecke bemerken wir, dass z entweder die Form $2u$, oder $2u + 1$ besitzen kann. Setzen wir beide Werthe ein, so erhalten wir für die gemeinsamen Theiler von

$$x^2 - 5 \, . \, 13y^2 \quad \text{und} \quad x^2 - 5y^2$$

die linearen Formen

$$520u + 1, 9, 29, 49, 51, 61, 69, 79, 81, 101, 121, 129, 131, 139, 159, 179, 181, 191, 199, 209, 211, 231, 251, 259, 261, 269, 289, 309, 311, 321, 329, 339, 341, 361, 381, 389, 391, 399, 419, 439, 441, 451, 459, 469, 471, 491, 511, 519.$$

Lässt man hier alle diejenigen weg, welche bei der Division durch 8 nicht den Rest 1, oder 7 geben, so verbleiben als gemeinsame Theiler der drei quadratischen Formen

$$x^2 - 5 \, . \, 13y^2, \quad x^2 - 5y^2, \quad x^2 - 2y^2$$

nur noch die linearen Formen

$$520u + 1, 9, 49, 79, 81, 121, 129, 159, 191, 199, 209, 231, 289, 311, 321, 329, 361, 391, 399, 439, 441, 471, 511, 519.$$

Es bleiben uns noch, für die Bestimmung der Theiler von 8520191, die vier quadratischen Formen

$$x^2-2.5y^2,\quad x^2-13y^2,\quad x^2-37y^2,\quad x^2-101y^2$$

übrig.

Von diesen haben die ersten zwei alle Theiler mit den obigen drei Formen

$$x^2-5.13y^2,\quad x^2-5y^2,\quad x^2-2y^2$$

gemeinschaftlich. Davon überzeugen wir uns durch die Bemerkung, dass die Theilbarkeit von

$$x_1^2-5.13y_1^2,\quad x_2^2-5y_2^2,\quad x_3^2-2y_3^2$$

durch p die Congruenzen

$$\left.\begin{aligned} x_1^2 &\equiv 5.13y_1^2 \\ x_2^2 &\equiv 5y_2^2 \\ x_3^2 &\equiv 2y_3^2 \end{aligned}\right\} \pmod{p},$$

also auch die Congruenzen

$$\left.\begin{aligned} x_1^2x_2^2 &\equiv 5^2.13y_1^2y_2^2 \\ x_2^2x_3^2 &\equiv 2.5y_2^2y_3^2 \end{aligned}\right\} \pmod{p}$$

ergiebt, was die Theilbarkeit von

$$x^2-13y^2 \quad \text{und} \quad x^2-2.5y^2$$

durch p aussagt.

Was aber die übrigen zwei Formen

$$x^2-37y^2;\quad x^2-101y^2$$

betrifft, so können wir ihre linearen Formen aufsuchen und dann aus den obengefundenen Formen

$520u+$ 1, 9, 49, 79, 81, 121, 129, 159, 191, 199, 209, 231, 289, 311, 321, 329, 361, 391, 399, 439, 441, 471, 511, 519,

diejenigen weglassen, welche mit den zuletzt aufgesuchten nicht übereinstimmen, um auf diese Weise die Anzahl der Formen, unter denen die Theiler von 8520191 zu suchen sind, noch zu verringern. Dazu müssen wir die gefundenen Formen so transformiren, dass der Coëfficient der Veränderlichen ein Vielfaches von 4.37 und 4.101 werde, um dann durch Division dieser Formen durch 4.37 und 4.101 zu erfahren, welche von diesen Formen unter

den linearen Formen der Theiler von x^2-37y^2, x^2-101y^2 zu finden sind. Auf diese Weise würden wir aber ausserordentlich viele lineare Formen für die Bestimmung der Theiler von 8520191 erhalten. Daher kürzen wir das Verfahren dadurch bedeutend ab, dass wir, bevor wir die Formen x^2-37y^2, x^2-101y^2 in Betracht ziehen, vorläufig bei den gemeinsamen Theilern der drei Formen

$$x^2-5\,.\,13y^2,\quad x^2-5y^2,\quad x^2-2y^2$$

verweilen, um zuerst unter diesen Theilern diejenigen *Primzahlen* aufzusuchen, welche kleiner als $\sqrt{8520191}$ sind. Wir finden folgende Zahlen:

79	521	719	919	1231	1511	1889	2129	2521	2791.
191	569	751	991	1249	1559	1951	2161	2551	
199	599	809	1031	1361	1609	1999	2239	2591	
311	601	881	1039	1439	1759	2081	2311	2609	
439	641	911	1049	1481	1871	2089	2441	2729	

Unter diesen Zahlen müssten wir den kleinsten Divisor von 8520191 suchen. Da die Anzahl dieser Zahlen bedeutend gross ist, so würde diese Arbeit ziemlich langwierig sein. Daher schliessen wir zuerst diejenigen Zahlen aus, welche keine Theiler der quadratischen Formen x^2-37y^2, x^2-101y^2 sein können.

Zu diesem Ende bemerken wir, dass die Theiler von x^2-37y^2, wie sie in den Tabellen zu finden sind, nach Division durch 148 die Reste

1, 3, 7, 9, 11, 21, 25, 27, 33, 41, 47, 49,
53, 63, 65, 67, 71, 73, 75, 77, 81, 83, 85, 95,
99, 101, 107, 115, 121, 123, 127, 137, 139, 141, 145, 147,

ergeben. Unter den obigen Primzahlen genügen dieser Bedingung nur folgende

521	751	1439	2081
599	881	1481	2441
601	1039	1871	2591
641	1231	1951	2729
719	1249	1999	2791.

In analoger Weise finden wir ferner, dass unter diesen Zahlen nur

521, 601, 1231, 1249, 1999, 2441, 2729, 2791

Theiler der quadratischen Form $x^2 - 101y^2$ sein können.

Indem wir 8520191 durch diese Zahlen zu dividiren versuchen, überzeugen wir uns, dass dieselben keine Theiler sind. Daraus folgt dass 8520191 eine Primzahl ist.

So sehen wir nun, wie man auf Grund der Theorie von den Theilern quadratischer Formen die Primzahlfactoren irgend einer gegebenen Zahl A finden kann, sobald man aus den Gleichungen

$$d_0 = 1, \quad d_1 = A - (E\sqrt{A})^2,$$

$$\sqrt{A - d_{n+1}d_n} = d_n E \frac{\sqrt{A - d_n d_{n-1}} + \sqrt{A}}{d_n} - \sqrt{A - d_n d_{n-1}}$$

eine genügende Reihe solcher Zahlen

$$d_0, \quad d_1, \quad d_2, \quad \ldots .$$

berechnet hat.

Anhang I.

Ueber quadratische Reste.

Wir haben in Kap. IV gesehen, wie man den Werth des Symbols $\left(\frac{a}{p}\right)$ bestimmen kann, um dadurch zu erfahren, ob die Congruenz

$$x^2 \equiv a \pmod{p}$$

eine Lösung hat, oder nicht.

Aber die Methode für die Bestimmung des Werthes von $\left(\frac{a}{p}\right)$ kann noch bedeutend vereinfacht werden; man kann nämlich den Werth dieses Symbols auch bestimmen, ohne die Zahl a, oder andere Zahlen in ihre Primzahlfactoren zu zerlegen. Eine solche Vereinfachung ist von besonderer Wichtigkeit, wenn a eine grosse Zahl ist; in diesem Falle wird die Zerlegung von a in Primzahlfactoren sehr beschwerlich und erfordert viel mehr Zeit, als die directe Bestimmung von $\left(\frac{a}{p}\right)$ nach der Methode, welche wir nunmehr zeigen wollen.

Nach *Legendre* bezeichneten wir mit dem Symbol $\left(\frac{a}{p}\right)$, wenn p eine ungerade Primzahl und kein Theiler von a ist, die Einheit mit positivem, oder negativem Vorzeichen, jenachdem in der Congruenz

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$$

das positive, oder negative Vorzeichen zu nehmen ist, damit diese Congruenz befriedigt werde. Wir wollen nunmehr, nach *Jacobi*, das Product mehrerer solcher Symbole

$$\left(\frac{a}{p_1}\right), \quad \left(\frac{a}{p_2}\right), \quad \left(\frac{a}{p_3}\right), \quad \ldots .$$

mit dem Symbol

$$\left(\frac{a}{p_1\, p_2\, p_3 \ldots .}\right)$$

bezeichnen.

Indem wir diese Bezeichnungsweise zulassen, erhalten wir in dem Symbol $\left(\frac{a}{N}\right)$, wenn N eine ungerade Zahl ist, das Product der Symbole

$$\left(\frac{a}{\alpha}\right), \quad \left(\frac{a}{\beta}\right), \quad \left(\frac{a}{\gamma}\right), \quad \ldots ., \quad \text{wobei } \alpha, \beta, \gamma, \ldots .$$

diejenigen Primzahlen bedeuten, welche in N enthalten sind. In dem Falle, dass N eine Primzahl ist, wird dieses *Jacobi*'sche Symbol $\left(\frac{a}{N}\right)$ mit dem *Legendre*'schen identisch und dasselbe entscheidet dann über die Möglichkeit oder Unmöglichkeit der Congruenz

$$x^2 \equiv a \pmod{N}.$$

Wir wollen nunmehr zeigen, dass *das Jacobi'sche Symbol* $\left(\frac{a}{N}\right)$ *ebenfalls alle diejenigen Gleichungen befriedigt, welche uns zur Bestimmung des Legendre'schen Symbols* $\left(\frac{a}{p}\right)$ *dienten, wenn p eine Primzahl ist.*

I. *Es ist* zunächst:

$$\left(\frac{a'.\,a''.\ldots.}{N}\right) = \left(\frac{a'}{N}\right)\left(\frac{a''}{N}\right) \ldots .$$

Denn man hat, wenn $\alpha, \beta, \gamma, \ldots .$ Primzahlen sind, die Gleichungen

$$\left(\frac{a'.a''....}{\alpha}\right)=\left(\frac{a'}{\alpha}\right)\left(\frac{a''}{\alpha}\right)....,$$

$$\left(\frac{a'.a''....}{\beta}\right)=\left(\frac{a'}{\beta}\right)\left(\frac{a''}{\beta}\right)....,$$

$$\left(\frac{a'.a''....}{\gamma}\right)=\left(\frac{a'}{\gamma}\right)\left(\frac{a''}{\gamma}\right)....,$$

$$....................,$$

deren gliedweise Multiplication die Gleichung

$$\left(\frac{a'a''...}{\alpha}\right)\left(\frac{a'a''...}{\beta}\right)\left(\frac{a'a''...}{\gamma}\right)....=$$

$$\left(\frac{a'}{\alpha}\right)\left(\frac{a'}{\beta}\right)\left(\frac{a'}{\gamma}\right)....\left(\frac{a''}{\alpha}\right)\left(\frac{a''}{\beta}\right)\left(\frac{a''}{\gamma}\right)....$$

ergiebt, welche nach unserer Bezeichnungsweise so geschrieben werden kann:

$$\left(\frac{a'a''...}{\alpha\beta\gamma...}\right)=\left(\frac{a'}{\alpha\beta\gamma...}\right)\left(\frac{a''}{\alpha\beta\gamma...}\right)....$$

Ist nun aber, wie wir voraussetzen,

$$N=\alpha\beta\gamma....,$$

so erhalten wir

$$\left(\frac{a'a''....}{N}\right)=\left(\frac{a'}{N}\right)\left(\frac{a''}{N}\right)....,$$

was wir beweisen wollten.

II. *Aus* I *folgt unmittelbar:*

$$\left(\frac{a'^2}{N}\right)=1$$

und somit

$$\left(\frac{a'^2.a''}{N}\right)=\left(\frac{a''}{N}\right).$$

Aus diesem Grunde kann man bei der Bestimmung des Werthes von $\left(\frac{a}{N}\right)$ alle in a enthaltenen quadratischen Factoren vernachlässigen.

III. *Ist*

$$a\equiv a'\ (\text{mod.}\ N),$$

so ist

$$\left(\frac{a}{N}\right) = \left(\frac{a'}{N}\right).$$

Denn aus $N = \alpha\,\beta\,\gamma\,\ldots$ und $a \equiv a'$ (mod. N) folgt:

$$a \equiv a' \text{ (mod. } \alpha\text{), also } \left(\frac{a}{\alpha}\right) = \left(\frac{a'}{\alpha}\right)$$

$$a \equiv a' \text{ (mod. } \beta\text{), } \quad „ \quad \left(\frac{a}{\beta}\right) = \left(\frac{a'}{\beta}\right)$$

$$a \equiv a' \text{ (mod. } \gamma\text{), } \quad „ \quad \left(\frac{a}{\gamma}\right) = \left(\frac{a'}{\gamma}\right)$$

$$\vdots \qquad\qquad\qquad \vdots$$

und somit durch Multiplication:

$$\left(\frac{a}{\alpha}\right)\left(\frac{a}{\beta}\right)\left(\frac{a}{\gamma}\right)\ldots\ldots = \left(\frac{a'}{\alpha}\right)\left(\frac{a'}{\beta}\right)\left(\frac{a'}{\gamma}\right)\ldots\ldots,$$

also, nach unserer Bezeichnung

$$\left(\frac{a}{\alpha\,\beta\,\gamma\ldots}\right) = \left(\frac{a'}{\alpha\,\beta\,\gamma\ldots}\right),$$

d. h. wenn $N = \alpha\,\beta\,\gamma\,\ldots$ gesetzt wird:

$$\left(\frac{a}{N}\right) = \left(\frac{a'}{N}\right).$$

Auf Grund dieser Eigenschaft kann man bei der Bestimmung des Werthes von $\left(\frac{a}{N}\right)$ die Zahl a ersetzen durch den Rest, welcher bei der Division von a durch N verbleibt, oder *durch den absolut kleinsten Rest von a in Bezug auf Modul N.*

IV. *Es ist ferner,* analog wie bei $\left(\frac{a}{p}\right)$, wenn p eine Primzahl ist, *auch allgemein:*

$$\left(\frac{1}{N}\right) = 1; \quad \left(\frac{-1}{N}\right) = (-1)^{\frac{N-1}{2}}.$$

Denn, ist $N = \alpha\,\beta\,\gamma\ldots.$, wobei $\alpha, \beta, \gamma, \ldots.$ Primzahlen sind, so wird

$$\left(\frac{1}{N}\right) = \left(\frac{1}{\alpha}\right)\left(\frac{1}{\beta}\right)\left(\frac{1}{\gamma}\right)\ldots\ldots = 1$$

und

$$\left(\frac{-1}{N}\right) = \left(\frac{-1}{\alpha}\right)\left(\frac{-1}{\beta}\right)\left(\frac{-1}{\gamma}\right)\ldots\ldots$$

$$= (-1)^{\frac{\alpha-1}{2}+\frac{\beta-1}{2}+\frac{\gamma-1}{2}+\ldots\ldots}.$$

Es ist aber

$$\frac{N-1}{2} = \frac{\alpha\,\beta\,\gamma\ldots\ldots-1}{2};$$

die linke Seite kann man offenbar auch so schreiben:

$$\frac{\left(2\,\frac{\alpha-1}{2}+1\right)\left(2\,\frac{\beta-1}{2}+1\right)\left(2\,\frac{\gamma-1}{2}+1\right)\ldots\ldots-1}{2}$$

und wenn man in diesem ausgerechneten Ausdrucke alle Glieder, welche den Factor 2 haben, vernachlässigt, so reducirt sich derselbe offenbar auf

$$\frac{\alpha-1}{2}+\frac{\beta-1}{2}+\frac{\gamma-1}{2}+\ldots\ldots$$

[Vgl. Seite 218].

Daraus folgt somit:

$$\left(\frac{-1}{N}\right) = (-1)^{\frac{N-1}{2}},$$

was wir beweisen wollten.

V. *Mit Berücksichtigung von*

$$\left(\frac{aa'}{N}\right) = \left(\frac{a}{N}\right)\left(\frac{a'}{N}\right)$$

folgt aus IV *unmittelbar:*

$$\left(\frac{-a}{N}\right) = \left(\frac{a}{N}\right)(-1)^{\frac{N-1}{2}}.$$

Mit Hülfe dieser gefundenen Eigenschaften sind wir nun im Stande eine Gleichung zwischen $\left(\frac{a}{N}\right)$ und $\left(\frac{N}{a}\right)$ zu finden, die analog ist derjenigen, welche zwischen $\left(\frac{a}{p}\right)$ und $\left(\frac{p}{a}\right)$ besteht im Falle, wenn a, p Primzahlen sind und dann das *Reciprocitätsgesetz* zweier Primzahlen genannt wird.

Es seien

$$N = \alpha\beta\gamma\ldots\ldots,\quad a = \alpha'\beta'\gamma'\ldots\ldots,$$

wobei $\alpha', \beta', \gamma', \ldots\ldots$ ebenso wie $\alpha, \beta, \gamma, \ldots\ldots$ ungerade Primzahlen sind. Nach dem Reciprocitätsgesetz der Primzahlen erhält man:

$$\left(\frac{\alpha'}{\alpha}\right) = \left(\frac{\alpha}{\alpha'}\right)(-1)^{\frac{\alpha-1}{2}\cdot\frac{\alpha'-1}{2}},$$

$$\left(\frac{\alpha'}{\beta}\right) = \left(\frac{\beta}{\alpha'}\right)(-1)^{\frac{\beta-1}{2}\cdot\frac{\alpha'-1}{2}},$$

$$\left(\frac{\alpha'}{\gamma}\right) = \left(\frac{\gamma}{\alpha'}\right)(-1)^{\frac{\gamma-1}{2}\cdot\frac{\alpha'-1}{2}},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

woraus durch Multiplication sich die Gleichung ergiebt:

$$\left(\frac{\alpha'}{\alpha}\right)\left(\frac{\alpha'}{\beta}\right)\left(\frac{\alpha'}{\gamma}\right)\ldots\ldots =$$

$$\left(\frac{\alpha}{\alpha'}\right)\left(\frac{\beta}{\alpha'}\right)\left(\frac{\gamma}{\alpha'}\right)\ldots\ldots(-1)^{\frac{\alpha'-1}{2}\left(\frac{\alpha-1}{2}+\frac{\beta-1}{2}+\frac{\gamma-1}{2}+\ldots\right)},$$

oder

$$\left(\frac{\alpha'}{\alpha\beta\gamma\ldots}\right) = \left(\frac{\alpha\beta\gamma\ldots}{\alpha'}\right)(-1)^{\frac{\alpha'-1}{2}\left(\frac{\alpha-1}{2}+\frac{\beta-1}{2}+\frac{\gamma-1}{2}+\ldots\right)}.$$

Es ist aber $\alpha\beta\gamma\ldots\ldots = N$ und

$$\frac{\alpha-1}{2}+\frac{\beta-1}{2}+\frac{\gamma-1}{2}+\ldots$$

unterscheidet sich von $\frac{N-1}{2}$, wie wir wiederholt bemerkt haben, um eine gerade Zahl, so dass die gefundene Gleichung in

$$\left(\frac{\alpha'}{N}\right) = \left(\frac{N}{\alpha'}\right)(-1)^{\frac{\alpha'-1}{2}\cdot\frac{N-1}{2}}$$

übergeht. In derselben Weise findet man:

$$\left(\frac{\beta'}{N}\right) = \left(\frac{N}{\beta'}\right)(-1)^{\frac{\beta'-1}{2}\cdot\frac{N-1}{2}},$$

$$\left(\frac{\gamma'}{N}\right) = \left(\frac{N}{\gamma'}\right)(-1)^{\frac{\gamma'-1}{2}\cdot\frac{N-1}{2}},$$

$$\cdots\cdots\cdots$$

und durch Multiplication:

$$\left(\frac{\alpha'}{N}\right)\left(\frac{\beta'}{N}\right)\left(\frac{\gamma'}{N}\right)\ldots\ldots =$$

$$\left(\frac{N}{\alpha'}\right)\left(\frac{N}{\beta'}\right)\left(\frac{N}{\gamma'}\right)\ldots(-1)^{\frac{N-1}{2}\left(\frac{\alpha'-1}{2}+\frac{\beta'-1}{2}+\frac{\gamma'-1}{2}+\ldots\right)}.$$

Durch analoge Bemerkungen, wie die obigen und Berücksichtigung des Werthes

$$\alpha'\,\beta'\,\gamma'\ldots = a$$

erhält man die Gleichung

$$\text{VI.}\qquad \left(\frac{a}{N}\right) = \left(\frac{N}{a}\right)(-1)^{\frac{N-1}{2}\cdot\frac{a-1}{2}},$$

welche das allgemeine Reciprocitätsgesetz irgend zweier ungerader Zahlen aussagt.

Es bleibt uns noch übrig eine Gleichung herzuleiten, welche den Werth von $\left(\frac{a}{N}\right)$ ergiebt, wenn $a = 2$ ist. Diese Gleichung kann man auf Grund der ebengefundenen Formeln direct, ohne Bezugnahme auf den Werth von $\left(\frac{2}{p}\right)$, wenn p eine Primzahl ist, herleiten.

Wir bemerken zu diesem Zwecke, dass aus

$$\left(\frac{a}{N}\right) = \left(\frac{N}{a}\right)(-1)^{\frac{N-1}{2}\cdot\frac{a-1}{2}},$$

wenn

$$a = 2n - 1, \quad N = 2n + 1$$

gesetzt wird, sich ergiebt:

$$\left(\frac{2n-1}{2n+1}\right) = \left(\frac{2n+1}{2n-1}\right)(-1)^{n(n-1)},$$

woraus folgt:

$$\left(\frac{2n-1}{2n+1}\right) = \left(\frac{2n+1}{2n-1}\right).$$

Es ist aber, nach III:

$$\left(\frac{2n-1}{2n+1}\right) = \left(\frac{2n-1-2n-1}{2n+1}\right) = \left(\frac{-2}{2n+1}\right) = \left(\frac{2}{2n+1}\right)(-1)^n$$

und

$$\left(\frac{2n+1}{2n-1}\right) = \left(\frac{2n+1-2n+1}{2n-1}\right) = \left(\frac{2}{2n-1}\right),$$

so dass aus der vorhergehenden Gleichung sich ergiebt:

$$\left(\frac{2}{2n+1}\right) : \left(\frac{2}{2n-1}\right) = (-1)^n.$$

Setzt man hierin für n successive die Werthe:

$$n = 2, 3, \ldots, \frac{N-1}{2}$$

und multiplicirt alle so erhaltenen Ergebnisse unter einander, so erhält man:

$$\left(\frac{2}{N}\right) = \left(\frac{2}{3}\right)(-1)^{2+3+\ldots+\frac{N-1}{2}}.$$

Da aber

$$\left(\frac{2}{3}\right) = -1$$

ist, so erhält man:

$$\left(\frac{2}{N}\right) = (-1)^{1+2+3+\ldots+\frac{N-1}{2}},$$

woraus sich sofort ergiebt:

$$\text{VII.} \qquad \left(\frac{2}{N}\right) = (-1)^{\frac{N^2-1}{8}}.$$

Auf Grund der eben hergeleiteten Gleichungen können wir uns des allgemeinen Symbols $\left(\frac{a}{N}\right)$ mit der zusammengesetzten Zahl N mit Vortheil bedienen, wenn es sich um die Bestimmung des Werthes von $\left(\frac{a}{p}\right)$ handelt, wobei p eine Primzahl bedeutet. Wir verfahren dabei folgendermassen:

Ist a grösser als p, so ersetzen wir das Symbol $\left(\frac{a}{p}\right)$ durch das andere Symbol $\left(\frac{r}{p}\right)$, wobei r den Rest der Division von a durch p bedeutet. (Anstatt des Restes der Division von a durch p, können wir auch den absolut kleinsten Rest von a nach Modul p nehmen). Ist r eine gerade Zahl, so zerlegen wir dieselbe in ein Product einer Potenz von 2 und einer ungeraden Zahl; dadurch wird der Werth des Symbols $\left(\frac{r}{p}\right)$ durch ein Product der Werthe der Symbole $\left(\frac{2}{p}\right)$ und $\left(\frac{r'}{p}\right)$ ausgedrückt. Die Symbole $\left(\frac{2}{p}\right)$ liefern, wenn ihrer eine gerade Anzahl vorhanden ist, ein Product, das den Werth 1 hat; tritt dagegen eine ungerade Anzahl derselben auf, so findet man ihren Werth aus der Gleichung

$$\left(\frac{2}{N}\right) = (-1)^{\frac{N^2-1}{8}}.$$

Wir wenden uns nunmehr zur Bestimmung des Symbols

$$\left(\frac{r'}{p}\right),$$

wobei $r' < p$ und r' ungerade ist.

Nach der oben hergeleiteten Gleichung

$$\left(\frac{a}{N}\right) = \left(\frac{N}{a}\right)(-1)^{\frac{N-1}{2}\cdot\frac{a-1}{2}}$$

ergiebt sich:

$$\left(\frac{r'}{p}\right) = \left(\frac{p}{r'}\right) (-1)^{\frac{r'-1}{2} \cdot \frac{p-1}{2}}.$$

Indem wir nun mit $\left(\frac{p}{r'}\right)$ ebenso verfahren, wie vorhin mit $\left(\frac{a}{p}\right)$, bewirken wir, dass die in dem Symbole auftretenden Zahlen immer kleiner und kleiner werden und kommen so endlich auf Symbole, deren Werthe sich unmittelbar durch die Gleichungen

$$\left(\frac{1}{N}\right) = 1; \quad \left(\frac{-1}{N}\right) = (-1)^{\frac{N-1}{2}}; \quad \left(\frac{2}{N}\right) = (-1)^{\frac{N^2-1}{8}}$$

bestimmen.

Dabei werden wir in $\left(\frac{a}{N}\right)$ die quadratischen Factoren, welche in a und in N enthalten sind, jedesmal weglassen können, wenn sich solche ohne besondere Mühe zu erkennen geben.

Beispiel. Man sucht den Werth des Symbols

$$\left(\frac{884257967}{2147483647}\right).$$

Hier ist die obere Zahl kleiner als die untere und beide sind ungerade. Auf Grund der Gleichung

$$\text{VI.} \qquad \left(\frac{a}{N}\right) = \left(\frac{N}{a}\right) (-1)^{\frac{N-1}{2} \cdot \frac{a-1}{2}}$$

erhalten wir daher:

$$\left(\frac{884\,257\,967}{2147\,483\,647}\right) = -\left(\frac{2147\,483\,647}{884\,257\,967}\right).$$

Da die Division von 2147 483 647 durch 884 257 967 den Rest 378 967 713 ergiebt, so erhalten wir:

$$\left(\frac{2147\,483\,647}{884\,257\,967}\right) = \left(\frac{378\,967\,713}{884\,257\,967}\right).$$

Auf Grund derselben Gleichung VI finden wir von Neuem

$$\left(\frac{378\,967\,713}{884\,257\,967}\right) = \left(\frac{884\,257\,967}{378\,967\,713}\right).$$

Da nun die Division von 884 257 967 durch 378 967 713 den Rest 126 322 541 liefert, so wird

$$\left(\frac{884\,257\,967}{378\,967\,713}\right) = \left(\frac{126\,322\,541}{378\,967\,713}\right).$$

In derselben Weise fortfahrend, finden wir:

$$\left(\frac{126\,322\,541}{378\,967\,713}\right) = \left(\frac{378\,967\,713}{126\,322\,541}\right) = \left(\frac{90}{126\,322\,541}\right),$$

$$\left(\frac{90}{126\,322\,541}\right) = \left(\frac{3}{126\,322\,541}\right)^2 \left(\frac{10}{126\,322\,541}\right)$$

$$= \left(\frac{10}{126\,322\,541}\right),$$

$$\left(\frac{10}{126\,322\,541}\right) = \left(\frac{2}{126\,322\,541}\right)\left(\frac{5}{126\,322\,541}\right).$$

Der Werth von $\left(\frac{2}{126\,322\,541}\right)$ ist nach der Formel

$$\left(\frac{2}{N}\right) = (-1)^{\frac{N^2-1}{8}}$$

gleich -1; folglich wird

$$\left(\frac{10}{126\,322\,541}\right) = -\left(\frac{5}{126\,322\,541}\right) =$$

$$-\left(\frac{126\,322\,541}{5}\right) = -\left(\frac{1}{5}\right) = -1.$$

Somit wird der Werth des gesuchten Symbols

$$\left(\frac{884\,257\,967}{2147\,483\,647}\right) = 1.$$

Würden wir den Werth dieses Symbols nach der im IVten Kapitel mitgetheilten Methode von Legender zu bestimmen gesucht haben, so müssten wir, bevor wir zu dieser Bestimmung schreiten, die Zahl 884 257 967 in Primzahlfactoren zerlegen, was mit grossen Schwierigkeiten verbunden wäre.

Mit eben solchem Vortheile kann man die von uns angenommene Bezeichnungsweise für das Product der Symbole

$$\left(\frac{a}{p_1}\right),\ \left(\frac{a}{p_2}\right),\ \left(\frac{a}{p_3}\right),\ \ldots.$$

und die auf Grund dieser Bezeichnung festgestellten Bedeutung des Symbols

$$\left(\frac{a}{N}\right),$$

wenn N eine zusammengesetzte Zahl ist, in der Theorie der Theiler der quadratischen Form

$$x^2 \pm ay^2$$

anwenden.

Hat z. B. die quadratische Form $x^2 - \varepsilon a y^2$, wobei $\varepsilon = \pm 1$ bedeutet, den Theiler N, wenn N ein Product der Primzahlen $\alpha, \beta, \gamma, \ldots$ ist, so bestehen die Gleichungen

$$\left(\frac{\varepsilon a}{\alpha}\right) = 1,\ \left(\frac{\varepsilon a}{\beta}\right) = 1,\ \left(\frac{\varepsilon a}{\gamma}\right) = 1,\ \ldots.$$

aus welchen folgt:

$$\left(\frac{\varepsilon a}{\alpha}\right)\left(\frac{\varepsilon a}{\beta}\right)\left(\frac{\varepsilon a}{\gamma}\right)\ldots. = 1,$$

was in unserer Bezeichnungsweise heisst:

$$\left(\frac{\varepsilon a}{N}\right) = 1.$$

Daraus folgt nach I:

$$\left(\frac{\varepsilon}{N}\right)\left(\frac{a}{N}\right) = 1.$$

Multiplicirt man diese Gleichung mit $\left(\frac{\varepsilon}{N}\right)$ und berücksichtigt, dass $\left(\frac{\varepsilon}{N}\right)^2 = 1$ wird, so erhält man

$$\left(\frac{a}{N}\right) = \left(\frac{\varepsilon}{N}\right).$$

Indem wir a als ungerade Zahl voraussetzen, haben wir aber, nach VI:

$$\left(\frac{N}{a}\right) = \left(\frac{a}{N}\right)(-1)^{\frac{a-1}{2} \cdot \frac{N-1}{2}},$$

woraus in Verbindung mit der letzten Gleichung sich ergiebt:

$$\left(\frac{N}{a}\right) = \left(\frac{\varepsilon}{N}\right)(-1)^{\frac{a-1}{2} \cdot \frac{N-1}{2}}.$$

Daraus folgt:

$$\left(\frac{N}{a}\right) = 1 \qquad \text{für } \varepsilon = 1 \text{ und } a = 4n+1,$$

$$\left(\frac{N}{a}\right) = (-1)^{\frac{N-1}{2}} \qquad ,, \ \varepsilon = 1 \ ,, \ a = 4n+3,$$

$$\left(\frac{N}{a}\right) = (-1)^{\frac{N-1}{2}} \qquad ,, \ \varepsilon = -1 \ ,, \ a = 4n+1,$$

$$\left(\frac{N}{a}\right) = 1 \qquad ,, \ \varepsilon = -1 \ ,, \ a = 4n+3.$$

Das sind somit die Gleichungen, denen die Theiler der quadratischen Form

$$x^2 \pm ay^2$$

genügen müssen. In diesen Gleichungen sind, im speciellen Falle, diejenigen enthalten, welche wir in Kapitel VII für die Bestimmung der Theiler von $x^2 \pm ay^2$ gefunden haben, wenn a eine Primzahl ist.

Anhang II.

Ueber die Bestimmung der primitiven Wurzeln.

In Kapitel VI haben wir zwei Methoden gezeigt, wie man die primitiven Wurzeln von Primzahlen bestimmen kann. Beide Methoden führen bei grossen Zahlen zu ungeheuren Rechnungen. Wir wollen nunmehr einige Lehrsätze beweisen, mit deren Hilfe man aus der Form gewisser Zahlen sofort ihre primitiven Wurzeln erkennen kann.

I. *Lehrsatz. Eine Primzahl von der Form* $2^{2n}+1$ *hat die primitive Wurzel 3.*

Beweis. Ist $p = 2^{2n}+1$, so ist $p-1$ nur durch 2 theilbar, daher wird eine Zahl a (nach Lehrsatz 48) primitive Wurzel von $2^{2n}+1$ sein, wenn die Congruenz

$$x^2 \equiv a \pmod{2^{2n}+1}$$

keine Lösung hat. Wir wollen nun beweisen, dass diese Congruenz für $a = 3$ keine Lösung besitzt. Zu diesem Zwecke bemerken wir, dass nach dem Reciprocitätsgesetz

$$\left(\frac{3}{2^{2n}+1}\right) = \left(\frac{2^{2n}+1}{3}\right)$$

ist. Die rechte Seite dieser Gleichung ist aber $\left(\frac{-1}{3}\right)$; denn, erhebt man beide Seiten der Congruenz $4 \equiv 1 \pmod{3}$ zur n^{ten} Potenz, so erhält man:

$$4^n \equiv 1 \pmod{3},$$

woraus erhellt, dass

$$(-1) \equiv 2^{2n} + 1 \pmod{3}.$$

Da aber $\left(\frac{-1}{3}\right) = -1$ ist, so wird auch $\left(\frac{3}{2^{2n}+1}\right) = -1$ und folglich kann die Congruenz

$$x^2 \equiv 3 \pmod{2^{2n} + 1}$$

keine Lösung besitzen und somit ist 3 primitive Wurzel von der Primzahl $2^{2n} + 1$.

Nach diesem Lehrsatze ist also 3 primitive Wurzel der Zahlen

$$5;\ 17;\ 257;\ 65537.$$

II. *Lehrsatz.* a) *Eine Primzahl von der Form*

$$p = 2(4n + 1) + 1 = 8n + 3$$

hat, wenn $4n + 1$ *eine Primzahl ist, die primitive Wurzel 2.*

b) *Eine Primzahl von der Form*

$$p = 2(4n + 3) + 1 = 8n + 7$$

hat, wenn $4n + 3$ *eine Primzahl ist, die primitive Wurzel*

$$2(4n + 3) - 1 = 8n + 5 = p - 2.$$

Beweis. Ist $p = 2(4n + 1) + 1$ und $4n + 1$ Primzahl, grösser als 1, so besteht $p - 1$ aus den zwei Primzahl-Factoren 2 und $4n + 1$; daher wird (nach Lehrsatz 48) a primitive Wurzel der Zahl $2(4n + 1) + 1$ sein, wenn keine der beiden Congruenzen

$$x^2 \equiv a;\quad x^{4n+1} \equiv a \pmod{2(4n + 1) + 1}$$

möglich ist. Wir wollen nun beweisen, dass diese Congruenzen für $a = 2$ keine Lösung zulassen. Die Unmöglichkeit der ersteren Congruenz, welche so lautet:

$$x^2 \equiv 2 \pmod{8n + 3},$$

geht aus Lehrsatz 32 unmittelbar hervor, wonach

$$\left(\frac{2}{8n + 3}\right) = -1$$

ist.

Was nun die zweite Congruenz

$$x^{4n+1} \equiv 2 \pmod{8n+3}$$

betrifft, so erhebe man beide Seiten derselben zum Quadrat und erhalte

$$x^{8n+2} \equiv 4 \pmod{8n+3}.$$

Dieser Congruenz kann offenbar keine Zahl genügen, die ein Vielfaches von $8n+3$ ist; ist aber x kein Vielfaches von $8n+3$, so ist nach dem *Fermat*'schen Satze:

$$x^{8n+2} \equiv 1 \pmod{8n+3},$$

so dass die vorhergehende Congruenz auf

$$4 \equiv 1 \pmod{8n+3},$$

oder

$$3 \equiv 0 \pmod{8n+3}$$

führen würde. Diese Congruenz könnte nur für $n = 0$ bestehen; den Fall $n = 0$, d. h. $4n+1 = 1$ haben wir aber ausgeschlossen. Folglich hat keine der Congruenzen

$$x^2 = a; \quad x^{4n+1} \equiv a \pmod{2(4n+1)+1}$$

für $a = 2$ und $n > 0$ eine Lösung und somit ist 2 primitive Wurzel von $2(4n+1)+1$, wenn $4n+1 > 1$ eine Primzahl ist.

[In dem bis jetzt ausgeschlossenen Falle $n = 0$ wird unsere Primzahl $8n+3 = 3$.

Da die Primzahl 3, wie unmittelbar zu sehen, die primitive Wurzel 2 besitzt, so gilt der Satz ohne Beschränkung für n, sobald nur $4n+1$ Primzahl ist].

Wir gehen jetzt zu dem zweiten Theile des Lehrsatzes über und nehmen an, es sei $p = 2(4n+3)+1$. Die Zahl $p-1$ besitzt dann die beiden Primzahlfactoren 2 und $4n+3$ und es wird eine Zahl a primitive Wurzel von $2(4n+3)+1$ sein, wenn keine der beiden Congruenzen

$$x^2 \equiv a; \quad x^{4n+3} \equiv a \pmod{8n+7}$$

besteht. Wir wollen beweisen, dass beide Congruenzen unmöglich sind, wenn $a = 2(4n+3)-1 = 8n+5$ ist.

Die Unmöglichkeit der ersteren Congruenz

$$x^2 \equiv 8n + 5 \pmod{8n + 7}$$

geht aus der Gleichung

$$\left(\frac{8n + 5}{8n + 7}\right) = \left(\frac{8n + 5 - 8n - 7}{8n + 7}\right) = \left(\frac{-2}{8n + 7}\right) = -1$$

(vgl. Lehrs. 32) unmittelbar hervor.

Die zweite Congruenz

$$x^{4n+3} \equiv 8n + 5 \pmod{8n + 7},$$

oder

$$x^{4n+3} \equiv -2 \pmod{8n + 7}$$

erhebe man zum Quadrat und berücksichtige, dass nach dem *Fermat*'schen Satze

$$x^{8n+6} \equiv 1 \pmod{8n + 7},$$

so dass

$$4 \equiv 1 \pmod{8n + 7}$$

sich ergeben würde, was nicht möglich ist. Folglich besitzt keine der Congruenzen

$$x^2 \equiv a; \quad x^{4n+3} \equiv a \pmod{2(4n + 3) + 1}$$

eine Lösung, wenn $a = 2(4n + 3) - 1$ gesetzt wird, und es ist somit $2(4n + 3) - 1$ primitive Wurzel der Zahl $2(4n + 3) + 1$, was zu beweisen war.

Es ist also, nach diesem Lehrsatze, 2 primitive Wurzel der Primzahlen

11; 59; 83; 107; 123.

Während

7	die	primitive	Wurzel	5	besitzt
23	„	„	„	21	„
47	„	„	„	45	„

etc.

III. *Lehrsatz. Eine Primzahl von der Form*

$$4N + 1,$$

hat, wenn N eine Primzahl und > 2 *ist, die primitive Wurzel* 2.

Beweis. Ist $p = 4N + 1$ und N eine Primzahl > 2, so enthält $p - 1$ nur die zwei Primzahlfactoren 2

und N; daher wird eine Zahl a primitive Wurzel von $4N+1$ sein, wenn keine der beiden Congruenzen

$$x^2 \equiv a; \quad x^N \equiv a \pmod{4N+1}$$

eine Lösung hat. Wir wollen nun beweisen, dass dieses zutrifft, wenn $a = 2$ gesetzt wird. Die erste Congruenz

$$x^2 \equiv 2 \pmod{4N+1}$$

kann nicht stattfinden, da N eine ungerade Zahl, also von der Form $N = 2n+1$, folglich $4N+1 = 8n+5$ ist und nach dem 32ten Lehrsatze

$$\left(\frac{2}{8n+5}\right) = -1$$

ist.

Was nun die zweite Congruenz

$$x^N \equiv 2 \pmod{4N+1}$$

betrifft, so erhebe man dieselbe auf die 4te Potenz und bemerke, dass aus derselben, mit Berücksichtigung der aus dem *Fermat*'schen Satze entspringenden Congruenz

$$x^{4N} \equiv 1 \pmod{4N+1}$$

sich die Congruenz $16 \equiv 1 \pmod{4N+1}$, oder

$$3 \,.\, 5 \equiv 0 \pmod{4N+1}$$

ergeben würde. Dieses ist offenbar unmöglich, da weder 3, noch 5 durch $4N+1$ für $N > 2$ theilbar sein kann.

Da nun keine der beiden Congruenzen

$$x^2 \equiv 2; \quad x^N \equiv 2 \pmod{4N+1}$$

bestehen kann, so ist 2, nach Lehrsatz 48, primitive Wurzel der Primzahl $4N+1$, wenn N eine Primzahl > 2 ist.

So haben die Primzahlen

13; 29; 53; 149; 173; 269; 293; 317; ....

die primitive Wurzel 2.

IV. Lehrsatz. *Eine Primzahl von der Form*

$$4 \,.\, 2^m N + 1,$$

hat, wenn N eine Primzahl,

$$N > \frac{9^{2^m}}{4 \cdot 2^m} \quad \textit{und} \quad m > 0$$

ist, die primitive Wurzel 3.

Beweis. Ist $p = 4 \cdot 2^m N + 1$ und N Primzahl, so enthält $p-1$ nur die Primzahlfactoren 2 und N und es wird a primitive Wurzel von p sein, wenn keine der beiden Congruenzen

$$x^2 \equiv a; \quad x^N \equiv a \pmod{p}$$

eine Lösung besitzt. Wir wollen nun zusehen, ob diese Congruenzen befriedigt werden können, wenn $a = 3$ und die Primzahl

$$N > \frac{9^{2^m}}{4 \cdot 2^m} \quad \text{und} \quad m > 0$$

ist.

Aus den letzten Ungleichungen ergiebt sich jedenfalls [*)]

$$N > 3,$$

so dass die Primzahl N, die nicht durch 3 theilbar sein kann, entweder die Gestalt $3n + 1$, oder $3n - 1$ haben muss. Es ist also

$$N \equiv \pm 1 \pmod{3}.$$

Erhebt man die Congruenz $2 \equiv -1 \pmod{3}$ auf die $(m + 2)$te Potenz und multiplicirt

$$2^{m+2} \equiv \pm 1 \pmod{3}$$

mit der letzten Congruenz für N, so erhält man für diese Primzahl die Congruenz

$$2^{m+2} N \equiv \pm 1 \pmod{3},$$

so dass eine der beiden Congruenzen

$$4 \cdot 2^m N + 1 \equiv 0 \pmod{3}; \text{ oder } 4 \cdot 2^m N + 1 \equiv 2 \pmod{3}$$

befriedigt werden müsste. Da aber die erste Congruenz

[*) Entwickelt man $9^{2^m} = (1 + 8)^{2^m}$ nach dem binomischen Satze, so betragen bereits die ersten drei der nur positiv auftretenden Glieder: $1 + 8 \cdot 2^m \cdot + (2^m - 1) \cdot 32 \cdot 2^m + \ldots$ für $m > 0$, also $2^m > 1$, mehr als $3(4 \cdot 2^m)$.]

für die Primzahl $4 \,.\, 2^m N + 1$ unmöglich ist, so bleibt nur die zweite übrig.

Aus

$$4 \,.\, 2^m N + 1 \equiv 2 \pmod{3},$$

folgt nun

$$\left(\frac{4 \,.\, 2^m N + 1}{3}\right) = \left(\frac{2}{3}\right) = -1;$$

da andererseits nach dem Reciprocitätsgesetz

$$\left(\frac{4 \,.\, 2^m N + 1}{3}\right) = \left(\frac{3}{4 \,.\, 2^m N + 1}\right)$$

ist, so ergiebt sich

$$\left(\frac{3}{4 \,.\, 2^m N + 1}\right) = -1,$$

woraus erhellt, dass die Congruenz

$$x^2 \equiv 3 \pmod{4 \,.\, 2^m N + 1}$$

unmöglich ist.

Es bleibt uns noch zu beweisen, dass auch die Congruenz

$$x^N \equiv 3 \pmod{4 \,.\, 2^m N + 1}$$

unter den gemachten Voraussetzungen nicht bestehen kann. Wir erheben, zu diesem Zwecke, beide Seiten dieser Congruenz auf die Potenz $4 \,.\, 2^m$ und mit Berücksichtigung der aus dem *Fermat*'schen Satze sich ergebenden Congruenz

$$x^{4 \,.\, 2^m N} \equiv 1 \pmod{4 \,.\, 2^m N + 1},$$

erhalten wir

$$3^{4 \,.\, 2^m} \equiv 1 \pmod{4 \,.\, 2^m N + 1},$$

woraus folgt:

$$(3^{2 \,.\, 2^m} + 1)\,(3^{2 \,.\, 2^m} - 1) \equiv 0 \pmod{4 \,.\, 2^m N + 1}.$$

Diese Congruenz ist aber unmöglich, da keine der beiden Zahlen

$$3^{2 \,.\, 2^m} + 1 = 9^{2^m} + 1; \quad 3^{2 \,.\, 2^m} - 1 = 9^{2^m} - 1$$

durch $4 \,.\, 2^m N + 1$ theilbar sein kann. Denn nach unserer Voraussetzung war

$$N > \frac{9^{2^m}}{4 \,.\, 2^m}, \quad \text{also} \quad 4 \,.\, 2^m N + 1 > 9^{2^m} + 1.$$

Es kann somit unter den gemachten Voraussetzungen keine der beiden Congruenzen

$$x^2 \equiv a; \quad x^N \equiv a \pmod{4 \,.\, 2^m N + 1}$$

bestehen, wenn $a = 3$ angenommen wird; folglich hat die Primzahl $4 \,.\, 2^m N + 1$ die primitive Wurzel 3.

So haben die Primzahlen

$$89; \quad 233; \quad 569; \quad 809; \quad 857$$

von der Form $8N + 1$ und ebenso die Primzahl 5009 von der Form $16N + 1$ die primitive Wurzel 3.

Es folgen hier:

[Ad (2) ist zu bemerken, dass diese Tabellen, die von Ostrogradsky herrühren (vgl. pag. 181), auch von Jacobi in seinen Canon arithmeticus aufgenommen worden sind. Auch die Druckfehler waren dieselben; sind aber hinterher von Jacobi alle verbessert worden. Nachzutragen ist zum Druckfehlerverzeichniss des Canon arithmeticus: pag. 222, $p = 25$, arg. 14 tab. Ind. loco 8 lege 6].

Tabelle aller Primzahlen,

welche 10000 nicht übertreffen.

2	**179**	**419**	**661**	**947**	**1229**	**1523**
3	181	421	673	953	1231	1531
5	191	431	677	967	1237	1543
7	193	433	683	971	1249	1549
11	197	439	691	977	1259	1553
13	199	443	701	983	1277	1559
17	211	449	709	991	1279	1567
19	223	457	719	997	1283	1571
23	227	461	727	1009	1289	1579
29	229	463	733	1013	1291	1583
31	**233**	**467**	**739**	**1019**	**1297**	**1597**
37	239	479	743	1021	1301	1601
41	241	487	751	1031	1303	1607
43	251	491	757	1033	1307	1609
47	257	499	761	1039	1319	1613
53	263	503	769	1049	1321	1619
59	269	509	773	1051	1327	1621
61	271	521	787	1061	1361	1627
67	277	523	797	1063	1367	1637
71	281	541	809	1069	1373	1657
73	**283**	**547**	**811**	**1087**	**1381**	**1663**
79	293	557	821	1091	1399	1667
83	307	563	823	1093	1409	1669
89	311	569	827	1097	1423	1693
97	313	571	829	1103	1427	1697
101	317	577	839	1109	1429	1699
103	331	587	853	1117	1433	1709
107	337	593	857	1123	1439	1721
109	347	599	859	1129	1447	1723
113	349	601	863	1151	1451	1733
127	**353**	**607**	**877**	**1153**	**1453**	**1741**
131	359	613	881	1163	1459	1747
137	367	617	883	1171	1471	1753
139	373	619	887	1181	1481	1759
149	379	631	907	1187	1483	1777
151	383	641	911	1193	1487	1783
157	389	643	919	1201	1489	1787
163	397	647	929	1213	1493	1789
167	401	653	937	1217	1499	1801
173	409	659	941	1223	1511	1811

Primzahlen unter 10000.

1823	**2131**	**2437**	**2749**	**3083**	**3433**	**3733**
1831	2137	2441	2753	3089	3449	3739
1847	2141	2447	2767	3109	3457	3761
1861	2143	2459	2777	3119	3461	3767
1867	2153	2467	2789	3121	3463	3769
1871	2161	2473	2791	3137	3467	3779
1873	2179	2477	2797	3163	3469	3793
1877	2203	2503	2801	3167	3491	3797
1879	2207	2521	2803	3169	3499	3803
1889	2213	2531	2819	3181	3511	3821
1901	**2221**	**2539**	**2833**	**3187**	**3517**	**3823**
1907	2237	2543	2837	3191	3527	4833
1913	2239	2549	2843	3203	3529	3847
1931	2243	2551	2851	3209	3533	3851
1933	2251	2557	2857	3217	3539	3853
1949	2267	2579	2861	3221	3541	3863
1951	2269	2591	2879	3229	3547	3877
1973	2273	2593	2887	3251	3557	3881
1979	2281	2609	2897	3253	3559	3889
1987	2287	2617	2903	3257	3571	3907
1993	**2293**	**2621**	**2909**	**3259**	**3581**	**3911**
1997	2297	2633	2917	3271	3583	3917
1999	2309	2647	2927	3299	3593	3919
2003	2311	2657	2939	3301	3607	3923
2011	2333	2659	2953	3307	3613	3929
2017	2339	2663	2957	3313	3617	3931
2027	2341	2671	2963	3319	3623	3943
2029	2347	2677	2969	3323	3631	3947
2039	2351	2683	2971	3329	3637	3967
2053	2357	2687	2999	3331	3643	3989
2063	**2371**	**2689**	**3001**	**3343**	**3659**	**4001**
2069	2377	2693	3011	3347	3671	4003
2081	2381	2699	3019	3359	3673	4007
2083	2383	2707	3023	3361	3677	4013
2087	2389	2711	3037	3371	3691	4019
2089	2393	2713	3041	3373	3697	4021
2099	2399	2719	3049	3389	3701	4027
2111	2411	2729	3061	3391	3709	4049
2113	2417	2731	3067	3407	3719	4051
2129	2423	2741	3079	3413	3727	4057

Primzahlen unter 10000.

4073	**4421**	**4759**	**5099**	**5449**	**5801**	**6143**
4079	4423	4783	5101	5471	5807	6151
4091	4441	4787	5107	5477	5813	6163
4093	4447	4789	5113	5479	5821	6173
4099	4451	4793	5119	5483	5827	6197
4111	4457	4799	5147	5501	5839	6199
4127	4463	4801	5153	5503	5843	6203
4129	4481	4813	5167	5507	5849	6211
4133	4483	4817	5171	5519	5851	6217
4139	4493	4831	5179	5521	5857	6221
4153	**4507**	**4861**	**5189**	**5527**	**5861**	**6229**
4157	4513	4871	5197	5531	5867	6247
4159	4517	4877	5209	5557	5869	6257
4177	4519	4889	5227	5563	5879	6263
4201	4523	4903	5231	5569	5881	6269
4211	4547	4909	5233	5573	5897	6271
4217	4549	4919	5237	5581	5903	6277
4219	4561	4931	5261	5591	5923	6287
4229	4567	4933	5273	5623	5927	6299
4231	4583	4937	5279	5639	5939	6301
4241	**4591**	**4943**	**5281**	**5641**	**5953**	**6311**
4243	4597	4951	5297	5647	5981	6317
4253	4603	4957	5303	5651	5987	6323
4259	4621	4967	5309	5653	6007	6329
4261	4637	4969	5323	5657	6011	6337
4271	4639	4973	5333	5659	6029	6343
4273	4643	4987	5347	5669	6037	6353
4283	4649	4993	5351	5683	6043	6359
4289	4651	4999	5381	5689	6047	6361
4297	4657	5003	5387	5693	6053	6367
4327	**4663**	**5009**	**5393**	**5701**	**6067**	**6373**
4337	4673	5011	5399	5711	6073	6379
4339	4679	5021	5407	5717	6079	6389
4349	4691	5023	5413	5737	6089	6397
4357	4703	5039	5417	5741	6091	6421
4363	4721	5051	5419	5743	6101	6427
4373	4723	5059	5431	5749	6113	6449
4391	4729	5077	5437	5779	6121	6451
4397	4733	5081	5441	5783	6131	6469
4409	4751	5087	5443	5791	6133	6473

Primzahlen unter 10000.

6481	**6841**	**7211**	**7573**	**7927**	**8293**	**8681**
6491	6857	7213	7577	7933	3297	8689
6521	6863	7219	7583	7937	8311	8693
6529	6869	7229	7589	7949	8317	8699
6547	6871	7237	7591	7951	8329	8707
6551	6883	7243	7603	7963	8353	8713
6553	6899	7247	7607	7993	8363	8719
6563	6907	7253	7621	8009	8369	8731
6569	6911	7283	7639	8011	8377	8737
6571	6917	7297	7643	8017	8387	8741
6577	**6947**	**7307**	**7649**	**8039**	**8389**	**8747**
6581	6949	7309	7669	8053	8419	8753
6599	6959	7321	7673	8059	8423	8761
6607	6961	7331	7681	8069	8429	8779
6619	6967	7333	7687	8081	8431	8783
6637	6971	7349	7691	8087	8443	8803
6653	6977	7351	7699	8089	8447	8807
6659	6983	7369	7703	8093	8461	8819
6661	6991	7393	7717	8101	8467	8821
6673	6997	7411	7723	8111	8501	8831
6679	**7001**	**7417**	**7727**	**8117**	**8513**	**8837**
6689	7013	7433	7741	8123	8521	8839
6691	7019	7451	7753	8147	8527	8849
6701	7027	7457	7757	8161	8537	8861
6703	7039	7459	7759	8167	8539	8863
6709	7043	7477	7789	8171	8543	8867
6719	7057	7481	7793	8179	8563	8887
6733	7069	7487	7817	8191	8573	8893
6737	7079	7489	7823	8209	8581	8923
6761	7103	7499	7829	8219	8597	8929
6763	**7109**	**7507**	**7841**	**8221**	**8599**	**8933**
6779	7121	7517	7853	8231	8609	8941
6781	7127	7523	7867	8233	8623	8951
6791	7129	7529	7873	8237	8627	8963
6793	7151	7537	7877	8243	8629	8969
6803	7159	7541	7879	8263	8641	8971
6823	7177	7547	7883	8269	8647	8999
6827	7187	7549	7901	8273	8663	9001
6829	7193	7559	7907	8287	8669	9007
6833	7207	7561	7919	8291	8677	9011

Primzahlen unter 10000.

9013	**9203**	**9391**	**9539**	**9739**	**9901**
9029	9209	9397	9547	9743	9907
9041	9221	9403	9551	9749	9923
9043	9227	9413	9587	9767	9929
9049	9239	9419	9601	9769	9931
9059	9241	9421	9613	9781	9941
9067	9257	9431	9619	9787	9949
9091	9277	9433	9623	9791	9967
9103	9281	9437	9629	9803	9973
9109	9283	9439	9631	9811	
9127	**9293**	**9461**	**9643**	**9817**	
9133	9311	9463	9649	9829	
9137	9319	9467	9661	9833	
9151	9323	9473	9677	9839	
9157	9337	9479	9679	9851	
9161	9341	9491	9689	9857	
9173	9343	9497	9697	9859	
9181	9349	9511	9719	9871	
9187	9371	9521	9721	9883	
9199	9377	9533	9733	9887	

Tabellen

der primitiven Wurzeln und der Indices aller Primzahlmoduln, welche 200 nicht übertreffen.

Primzahl 3. Primitive Wurzel 2. *Basis 2.*

I.

N.	1	2
	0	1

N.

I.	0	1
	1	2

Primzahl 5. Primitive Wurzeln 2, 3. *Basis 2.*

I.

N.	1	2	3	4
	0	1	3	2

N.

I.	0	1	2	3
	1	2	4	3

Primzahl 7. Primitive Wurzeln 3, 5. *Basis 3.*

I.

N.	1	2	3	4	5	6
	0	2	1	4	5	3

N.

I.	0	1	2	3	4	5
	1	3	2	6	4	5

Primzahl 11. Primitive Wurzeln 2, 6, 7, 8. *Basis 2.*

I.

N.	1	2	3	4	5	6	7	8	9	10
	0	1	8	2	4	9	7	3	6	5

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	2	4	8	5	10	9	7	3	6

Primzahl 13. Primitive Wurzeln 2, 6, 7, 11. *Basis 6.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	5	8	10	9	1	7	3	4
1	2	11	6							

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	6	10	8	9	2	12	7	3	5
1	4	11								

Primzahl 17. Primitive Wurzeln 3, 5, 6, 7, 10, 11, 12, 14. *Basis 10.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	10	11	4	7	5	9	14	6
1	1	13	15	12	3	3	8			

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	10	15	14	4	6	9	5	16	7
1	2	3	13	11	8	12				

Primzahl 19. Primitive Wurzeln 2, 3, 10, 13, 14, 15. *Basis 10.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	17	5	16	2	4	12	15	10
1	1	6	3	13	11	7	14	8	9	

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	10	5	12	6	3	11	15	17	18
1	9	14	7	13	16	8	4	2		

Primzahl 23. Primitive Wurzeln 5, 7, 10, 11, 14, 15, 17, 19, 20, 21.
Basis 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	8	20	16	15	6	21	2	18
1	1	3	14	12	7	13	10	17	4	5
2	9	19	11							

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	10	8	11	18	19	6	14	2	20
1	16	22	13	15	12	5	4	17	9	21
2	3	7								

Primzahl 29. Primitive Wurzeln 2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27. *Basis 10.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	11	27	22	18	10	20	5	26
1	1	23	21	2	3	17	16	7	9	15
2	12	19	6	24	4	8	13	25	14	

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	10	13	14	24	8	22	17	25	18
1	6	2	20	26	28	19	16	15	5	21
2	7	12	4	11	23	27	9	3		

Primzahl 31. Primitive Wurzeln 3, 11, 12, 13, 17, 21, 22, 24.
Basis 17.

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	12	13	24	20	25	4	6	26
1	2	29	7	23	16	3	18	1	8	22
2	14	17	11	21	19	10	5	9	28	27
3	15									

N.

I.	0	1	2	3	4	5	6	7	8	9
0	1	17	10	15	7	26	8	12	18	27
1	25	22	2	3	20	30	14	21	16	24
2	5	23	19	13	4	6	9	29	28	11

Primzahl 37. Primitive Wurzeln 2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35. *Basis 5.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	11	34	22	1	9	28	33	32
1	12	6	20	13	3	35	8	5	7	25
2	23	26	17	21	31	2	24	30	14	15
3	10	27	19	4	16	29	18			

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	5	25	14	33	17	11	18	16	6
1	30	2	10	13	28	29	34	22	36	32
2	12	23	4	20	26	19	21	31	7	35
3	27	24	9	8	3	15				

Primzahl 41. Primitive Wurzeln 6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35. *Basis 6.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7

Primzahl 43. Primitive Wurzeln 3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34. *Basis 28.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	39	17	36	5	14	7	33	34
1	2	6	11	40	4	22	30	16	31	29
2	41	24	3	20	8	10	37	9	1	25
3	19	32	27	23	13	12	28	35	26	15
4	38	18	21							

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	28	10	22	14	5	11	7	24	27
1	25	12	35	34	6	39	17	3	41	30
2	23	42	15	33	21	29	38	32	36	19
3	16	18	31	8	9	37	4	26	40	2
4	13	20								

Primzahl 47. Primitive Wurzeln 5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45. *Basis 10.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	30	18	14	17	2	38	44	36
1	1	27	32	3	22	35	28	42	20	29
2	31	10	11	39	16	34	33	8	6	43
3	19	5	12	45	26	9	4	24	13	21
4	15	25	40	37	41	7	23			

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	10	6	13	36	31	28	45	27	35
1	21	22	32	38	4	40	24	5	3	30
2	18	39	14	46	37	41	34	11	16	19
3	2	20	12	26	25	15	9	43	7	23
4	42	44	17	29	8	33				

Primzahl 53. Primitive Wurzeln 2, 3, 5, 8, 12, 14, 18, 19, 20, 21, 22, 26, 27, 31, 32, 33, 34, 35, 39, 41, 45, 48, 50, 51. *Basis 26.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	25	9	50	31	34	38	23	18
1	4	46	7	28	11	40	48	42	43	41
2	29	47	19	39	32	10	1	27	36	6
3	13	45	21	3	15	17	16	22	14	37
4	2	33	20	30	44	49	12	8	5	24
5	35	51	26							

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	26	40	33	10	48	29	12	47	3
1	25	14	46	30	38	34	36	35	9	22
2	42	32	37	8	49	2	52	27	13	20
3	43	5	24	41	6	50	28	39	7	23
4	15	19	17	18	44	31	11	21	16	45
5	4	51								

Primzahl 59. Primitive Wurzeln 2, 6, 8, 10, 11, 13, 14, 18, 23, 24, 30, 31, 32, 33, 34, 37, 38, 39, 40, 42, 43, 44, 47, 50, 52, 54, 55, 57. *Basis 10.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	25	32	50	34	57	44	17	6
1	1	45	24	23	11	8	42	14	31	22
2	26	18	12	27	49	10	48	38	36	4
3	33	7	9	19	39	20	56	41	47	55
4	51	2	43	13	37	40	52	53	16	30
5	35	46	15	28	5	21	3	54	29	

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	10	41	56	29	54	9	31	15	32
1	25	14	22	43	17	52	48	8	21	33
2	35	55	19	13	12	2	20	23	53	58
3	49	18	3	30	5	50	28	44	27	34
4	45	37	16	42	7	11	51	38	26	24
5	4	40	46	47	57	39	36	6		

Primzahl 61. Primitive Wurzeln 2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55, 59. *Basis 10.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	47	42	34	14	29	23	21	24
1	1	45	16	20	10	56	8	49	11	22
2	48	5	32	39	3	28	7	6	57	25
3	43	13	55	27	36	37	58	33	9	2
4	35	18	52	41	19	38	26	40	50	46
5	15	31	54	51	53	59	44	4	12	17
6	30									

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	10	39	24	57	21	27	26	16	38
1	14	18	58	31	5	50	12	59	41	44
2	13	8	19	7	9	29	46	33	25	6
3	60	51	22	37	4	40	34	35	45	23
4	47	43	3	30	56	11	49	2	20	17
5	48	53	42	54	52	32	15	28	36	55

Primzahl 67. Primitive Wurzeln 2, 7, 11, 12, 13, 18, 20, 28, 31, 32, 34, 41, 44, 46, 48, 50, 51, 57, 61, 63. *Basis 12.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	29	9	58	39	38	7	21	18
1	2	61	1	23	36	48	50	8	47	26
2	31	16	24	20	30	12	52	27	65	22
3	11	43	13	4	37	46	10	44	55	32
4	60	19	45	63	53	57	49	64	59	14
5	41	17	15	3	56	34	28	35	51	54
6	40	5	6	25	42	62	33			

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	12	10	53	33	61	62	7	17	3
1	36	30	25	32	49	52	21	51	9	41
2	23	8	29	13	22	63	19	27	56	2
3	24	20	39	66	55	57	14	34	6	5
4	60	50	64	31	37	42	35	18	15	46
5	16	58	26	44	59	38	54	45	4	48
6	40	11	65	43	47	28				

Primzahl 71. Primitive Wurzeln 7, 11, 13, 21, 22, 28, 31, 33, 35, 42, 44, 47, 52, 53, 55, 56, 59, 61, 62, 63, 65, 67, 68, 69. *Basis 62.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	58	18	46	14	6	33	34	36
1	2	43	64	27	21	32	22	7	24	38
2	60	51	31	5	52	28	15	54	9	4
3	20	13	10	61	65	47	12	30	26	45
4	48	55	39	44	19	50	63	17	40	66
5	16	25	3	59	42	57	67	56	62	29
6	8	37	1	69	68	41	49	11	53	23
7	35									

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	62	10	52	29	23	6	17	60	28
1	32	67	36	31	5	26	50	47	3	44
2	30	14	16	69	18	51	38	13	25	59
3	37	22	15	7	8	70	9	61	19	42
4	48	65	54	11	43	39	4	35	40	66
5	45	21	24	68	27	41	57	55	2	53
6	20	33	58	46	12	34	49	56	64	63

Primzahl 73. Primitive Wurzeln 5, 11, 13, 14, 15, 20, 26, 28, 29, 31, 33, 34, 39, 40, 42, 44, 45, 47, 53, 58, 59, 60, 62, 68. *Basis 5.*

I.

N	0	1	2	3	4	5	6	7	8	9
		0	8	6	16	1	14	33	24	12
1	9	55	22	59	41	7	32	21	20	62
2	17	39	63	46	30	2	67	18	49	35
3	15	11	40	61	29	34	28	64	70	65
4	25	4	47	51	71	13	54	31	38	66
5	10	27	3	53	26	56	57	68	43	5
6	23	58	19	45	48	60	69	50	37	52
7	42	44	36							

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	5	25	52	41	59	3	15	2	10
1	50	31	9	45	6	30	4	20	27	62
2	18	17	12	60	8	40	54	51	36	34
3	24	47	16	7	35	29	72	68	48	21
4	32	14	70	58	71	63	23	42	64	28
5	67	43	69	53	46	11	55	56	61	13
6	65	33	19	22	37	39	49	26	57	66
7	38	44								

Primzahl 79. Primitive Wurzeln 3, 6, 7, 28, 29, 30, 34, 35, 37, 39, 43, 47, 48, 53, 54, 59, 60, 63, 66, 68, 70, 74, 75, 77. *Basis 29.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	50	71	22	34	43	19	72	64
1	6	70	15	74	69	27	44	9	36	10
2	56	12	42	52	65	68	46	57	41	1
3	77	76	16	63	59	53	8	23	60	67
4	28	21	62	47	14	20	24	55	37	38
5	40	2	18	7	29	26	13	3	51	17
6	49	75	48	5	66	30	35	54	31	45
7	25	33	58	4	73	61	32	11	39	

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	29	51	57	73	63	10	53	36	17
1	19	77	21	56	44	12	32	59	52	7
2	45	41	4	37	46	70	55	15	40	54
3	65	68	76	71	5	66	18	48	49	78
4	50	28	22	6	16	69	26	43	62	60
5	2	58	23	35	67	47	20	27	72	34
6	38	75	42	33	9	24	64	39	25	14
7	11	3	8	74	13	61	31	30		

Primzahl 83. Primitive Wurzeln 2, 5, 6, 8, 13, 14, 15, 18, 19, 20, 22, 24, 32, 34, 35, 39, 42, 43, 45, 46, 47, 50, 52, 53, 54, 55, 56, 57, 58, 60, 62, 66, 67, 71, 72, 73, 74, 76, 79, 80. *Basis 50.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	3	52	6	81	55	24	9	22
1	2	72	58	67	27	51	12	4	25	59
2	5	76	75	16	61	80	70	74	30	36
3	54	32	15	42	7	23	28	60	62	37
4	8	38	79	49	78	21	19	69	64	48
5	1	56	73	13	77	71	33	29	39	20
6	57	34	35	46	18	66	45	53	10	68
7	26	17	31	43	63	50	65	14	40	47
8	11	44	41							

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	50	10	2	17	20	4	34	40	8
1	68	80	16	53	77	32	23	71	64	46
2	59	45	9	35	7	18	70	14	36	57
3	28	72	31	56	61	62	29	39	41	58
4	78	82	33	73	81	66	63	79	49	43
5	75	15	3	67	30	6	51	60	12	19
6	37	24	38	74	48	76	65	13	69	47
7	26	55	11	52	27	22	21	54	44	42
8	25	5								

Primzahl 89. Primitive Wurzeln 3, 6, 7, 13, 14, 15, 19, 23, 24, 26, 27, 28, 29, 30, 31, 33, 35, 38, 41, 43, 46, 48, 51, 54, 56, 58, 59, 60, 61, 62, 63, 65, 66, 70, 74, 75, 76, 82, 83, 86. *Basis 30.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	72	87	56	18	71	7	40	86
1	2	4	55	65	79	17	24	82	70	53
2	74	6	76	31	39	36	49	85	63	29
3	1	57	8	3	66	25	54	77	37	64
4	58	67	78	59	60	16	15	34	23	14
5	20	81	33	10	69	22	47	52	13	45
6	73	19	41	5	80	83	75	32	50	30
7	9	26	38	68	61	35	21	11	48	46
8	42	84	51	27	62	12	43	28	44	

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	30	10	33	11	63	21	7	32	70
1	53	77	85	58	49	46	45	15	5	61
2	50	76	55	48	16	35	71	83	87	29
3	69	23	67	52	47	75	25	38	72	24
4	8	62	80	86	88	59	79	56	78	26
5	68	82	57	19	36	12	4	31	40	43
6	44	74	84	28	39	13	34	41	73	54
7	18	6	2	60	20	66	22	37	42	14
8	64	51	17	65	81	27	9	3		

Primzahl 97. Primitive Wurzeln 5, 7, 10, 13, 14, 15, 17, 21, 23, 26, 29, 37, 38, 39, 40, 41, 56, 57, 58, 59, 60, 68, 71, 74, 76, 80, 82, 83, 84, 87, 90, 92. *Basis 10.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	86	2	76	11	88	53	66	4
1	1	82	78	83	43	13	56	19	90	27
2	87	55	72	79	68	22	73	6	33	47
3	3	26	46	84	9	64	80	41	17	85
4	77	71	45	44	62	15	69	60	58	10
5	12	21	63	14	92	93	23	29	37	65
6	89	32	16	57	36	94	74	51	95	81
7	54	25	70	20	31	24	7	39	75	42
8	67	8	61	91	35	30	34	49	52	18
9	5	40	59	28	50	38	48			

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	10	3	30	9	90	27	76	81	34
1	49	5	50	15	53	45	62	38	89	17
2	73	51	25	56	75	71	31	19	93	57
3	85	74	61	28	86	84	64	58	95	77
4	91	37	79	14	43	42	32	29	96	87
5	94	67	88	7	70	21	16	63	48	92
6	47	82	44	52	35	59	8	80	24	46
7	72	41	22	26	66	78	4	40	12	23
8	36	69	11	13	33	39	2	20	6	60
9	18	83	54	55	65	68				

Primzahl 101. Primitive Wurzeln 2, 3, 7, 8, 11, 12, 15, 18, 26, 27, 28, 29, 34, 35, 38, 40, 42, 46, 48, 50, 51, 53, 55, 59, 61, 63, 66, 67, 72, 73, 74, 75, 83, 86, 89, 90, 93, 94, 98, 99. *Basis 2.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	1	69	2	24	70	9	3	38
1	25	13	71	66	10	93	4	30	39	96
2	26	78	14	86	72	48	67	7	11	91
3	94	84	5	82	31	33	40	56	97	35
4	27	45	79	42	15	62	87	58	73	18
5	49	99	68	23	8	37	12	65	92	29
6	95	77	85	47	6	90	83	81	32	55
7	34	44	41	61	57	17	98	22	36	64
8	28	76	46	89	80	54	43	60	16	21
9	63	75	88	53	59	20	74	52	19	51
10	50									

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	2	4	8	16	32	64	27	54	7
1	14	28	56	11	22	44	88	75	49	98
2	95	89	77	53	5	10	20	40	80	59
3	17	34	68	35	70	39	78	55	9	18
4	36	72	43	86	71	41	82	63	25	50
5	100	99	97	93	85	69	37	74	47	94
6	87	73	45	90	79	57	13	26	52	3
7	6	12	24	48	96	91	81	61	21	42
8	84	67	33	66	31	62	23	46	92	83
9	65	29	58	15	30	60	19	38	76	51

Primzahl 103. Primitive Wurzeln 5, 6, 11, 12, 20, 21, 35, 40, 43, 44, 45, 48, 51, 53, 54, 62, 65, 67, 70, 71, 74, 75, 77, 78, 84, 85, 86, 87, 88, 96, 99, 101. *Basis 6.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		102	46	57	92	59	1	32	36	12
1	3	29	47	66	78	14	82	50	58	28
2	49	89	75	90	93	16	10	69	22	76
3	60	99	26	86	96	91	2	81	74	21
4	95	94	33	55	19	71	34	17	37	64
5	62	5	56	11	13	88	68	85	20	70
6	4	84	43	44	72	23	30	53	40	45
7	35	77	48	9	25	73	18	61	67	42
8	39	24	38	100	79	7	101	31	65	27
9	15	98	80	54	63	87	83	52	8	41
10	6	97	51							

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	6	36	10	60	51	100	85	98	73
1	26	53	9	54	15	90	25	47	76	44
2	58	39	28	65	81	74	32	89	19	11
3	66	87	7	42	46	70	8	48	82	80
4	68	99	79	62	63	69	2	12	72	20
5	17	102	97	67	93	43	52	3	18	5
6	30	77	50	94	49	88	13	78	56	27
7	59	45	64	75	38	22	29	71	14	84
8	92	37	16	96	61	57	33	95	55	21
9	23	35	4	24	41	40	34	101	91	31
10	83	86								

Primzahl 107. Primitive Wurzeln 2, 5, 6, 7, 8, 15, 17, 18, 20, 21, 22, 24, 26, 28, 31, 32, 38, 43, 45, 46, 50, 51, 54, 55, 58, 59, 60, 63, 65, 66, 67, 68, 70, 71, 72, 73, 74, 77, 78, 80, 82, 84, 88, 91, 93, 94, 95, 96, 97, 98, 103, 104. *Basis 63.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	95	78	84	13	67	57	73	50
1	2	76	56	58	46	91	62	105	39	96
2	97	29	65	60	45	26	47	22	35	72
3	80	21	51	48	94	70	28	6	85	30
4	86	90	18	93	54	63	49	16	34	8
5	15	77	36	64	11	89	24	68	61	87
6	69	102	10	1	40	71	37	33	83	32
7	59	81	17	41	101	104	74	27	19	88
8	75	100	79	98	7	12	82	44	43	92
9	52	9	38	99	5	3	23	55	103	20
10	4	14	66	31	25	42	53			

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	63	10	95	100	94	37	84	49	91
1	62	54	85	5	101	50	47	72	42	78
2	99	31	27	96	56	104	25	77	36	21
3	39	103	69	67	48	28	52	66	92	18
4	64	73	105	88	87	24	14	26	33	46
5	9	32	90	106	44	97	12	7	13	70
6	23	58	16	45	53	22	102	6	57	60
7	35	65	29	8	76	80	11	51	3	82
8	30	71	86	68	4	38	40	59	79	55
9	41	15	89	43	34	2	19	20	83	93
10	81	74	61	98	75	17				

Primzahl 109. Primitive Wurzeln 6, 10, 11, 13, 14, 18, 24, 30, 37, 39, 40, 42, 44, 47, 50, 51, 52, 53, 56, 57, 58, 59, 62, 65, 67 ,69, 70, 72, 79, 85, 91, 95, 96, 98, 99, 103. *Basis 10.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	93	28	78	16	13	88	63	56
1	1	107	106	7	73	44	48	21	41	3
2	94	8	92	105	91	32	100	84	58	10
3	29	74	33	27	6	104	26	65	96	35
4	79	45	101	66	77	72	90	5	76	68
5	17	49	85	97	69	15	43	31	103	71
6	14	22	59	36	18	23	12	47	99	25
7	89	42	11	80	50	60	81	87	20	83
8	64	4	30	46	86	37	51	38	62	40
9	57	95	75	102	98	19	61	52	53	55
10	2	9	34	67	70	24	82	39	54	

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	10	100	19	81	47	34	13	21	101
1	29	72	66	6	60	55	5	50	64	95
2	78	17	61	65	105	66	36	33	3	30
3	82	57	25	32	102	39	63	85	87	107
4	89	18	71	56	15	41	83	67	16	51
5	74	86	97	98	108	99	9	90	28	62
6	75	96	88	8	80	37	43	103	49	54
7	104	59	45	14	31	92	48	44	4	40
8	73	76	106	79	27	52	84	77	7	70
9	46	24	22	2	20	91	38	53	94	68
10	26	42	93	58	35	23	12	11		

Primzahl 113. Primitive Wurzeln 3, 5, 6, 10, 12, 17, 19, 20, 21, 23, 24, 27, 29, 33, 34, 37, 38, 39, 43, 45, 46, 47, 54, 55, 58, 59, 66, 67, 68, 70, 74, 75, 76, 79, 80, 84, 86, 89, 90, 92, 93, 94, 96, 100, 103, 107, 108, 110. *Basis 10.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	52	79	104	61	19	72	44	46
1	1	22	71	58	12	28	96	59	98	93
2	53	39	74	103	11	10	110	13	64	87
3	80	30	36	101	111	21	38	29	33	25
4	105	34	91	17	14	107	43	97	63	32
5	62	26	50	76	65	83	4	60	27	9
6	20	106	82	6	88	7	41	99	51	70
7	73	35	90	49	81	89	85	94	77	55
8	45	92	86	24	31	8	69	54	66	67
9	47	18	95	109	37	42	3	40	84	68
10	2	15	78	57	102	100	16	75	5	48
11	23	108	56							

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	10	100	96	56	108	63	65	85	59
1	25	24	14	27	44	101	106	43	91	6
2	60	35	11	110	83	39	51	58	15	37
3	31	84	49	38	41	71	32	94	36	21
4	97	66	95	46	8	80	9	90	109	73
5	52	68	2	20	87	79	112	103	13	17
6	57	5	50	48	28	54	88	89	99	86
7	69	12	7	70	22	107	53	78	102	3
8	30	74	62	55	98	76	82	29	64	75
9	72	42	81	19	77	92	16	47	18	67
10	105	33	104	23	4	40	61	45	111	93
11	26	34								

Primzahl 127. Primitive Wurzeln 3, 6, 7, 12, 14, 23, 29, 39, 43, 45, 46, 48, 53, 55, 56, 57, 58, 65, 67, 78, 83, 85, 86, 91, 92, 93, 96, 97, 101, 106, 109, 110, 112, 114, 116, 118. *Basis 109.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	18	23	36	111	41	125	54	46
1	3	52	59	20	17	8	72	118	64	42
2	21	22	70	11	77	96	38	69	35	79
3	26	50	90	75	10	110	82	112	60	43
4	39	76	40	121	88	31	29	120	95	124
5	114	15	56	67	87	37	53	65	97	91
6	44	30	68	45	108	5	93	107	28	34
7	2	116	100	24	4	119	78	51	61	32
8	57	92	94	25	58	103	13	102	106	123
9	49	19	47	73	12	27	113	89	16	98
10	6	101	33	14	74	7	85	84	105	1
11	55	9	71	80	83	122	115	66	109	117
12	62	104	48	99	86	81	63			

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	109	70	10	74	65	100	105	15	111
1	34	23	94	86	103	51	98	14	2	91
2	13	20	21	3	73	83	30	95	68	46
3	61	45	79	102	69	28	4	55	26	40
4	42	6	19	39	60	63	9	92	122	90
5	31	77	11	56	8	110	52	80	84	12
6	38	78	120	126	18	57	117	53	62	27
7	22	112	16	93	104	33	41	24	76	29
8	113	125	36	114	107	106	124	54	44	97
9	32	59	81	66	82	48	25	58	99	123
10	72	101	87	85	121	108	88	67	64	118
11	35	5	37	96	50	116	71	119	17	75
12	47	43	115	89	49	7				

Primzahl 131. Primitive Wurzeln 2, 6, 8, 10, 14, 17, 22, 23, 26, 29, 30, 31, 37, 40, 50, 54, 56, 57, 66, 67, 72, 76, 82, 83, 85, 87, 88, 90, 93, 95, 96, 97, 98, 103, 104, 106, 110, 111, 115, 116, 118, 119, 120, 122, 124, 126, 127, 128. *Basis 10.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	83	126	36	48	79	38	119	122
1	1	98	32	64	121	44	72	59	75	45
2	84	34	51	89	115	96	17	118	74	73
3	127	67	25	94	12	86	28	23	128	60
4	37	58	117	22	4	40	42	5	68	76
5	49	55	100	78	71	16	27	41	26	46
6	80	104	20	30	108	112	47	43	95	85
7	39	15	111	91	106	92	81	6	13	35
8	120	114	11	3	70	107	105	69	87	52
9	123	102	125	63	88	93	21	77	29	90
10	2	62	8	9	53	82	31	50	24	116
11	99	19	110	10	124	7	109	56	129	97
12	33	66	57	54	103	14	113	101	61	18
13	65									

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	10	100	83	44	47	77	115	102	103
1	113	82	34	78	125	71	55	26	129	111
2	62	96	43	37	108	32	58	56	36	98
3	63	106	12	120	21	79	4	40	7	70
4	45	57	46	67	15	19	59	66	5	50
5	107	22	89	104	123	51	117	122	41	17
6	39	128	101	93	13	130	121	31	48	87
7	84	54	16	29	28	18	49	97	53	6
8	60	76	105	2	20	69	35	88	94	23
9	99	73	75	95	33	68	25	119	11	110
10	52	127	91	124	61	86	74	85	64	116
11	112	72	65	126	81	24	109	42	27	8
12	80	14	9	90	114	92	3	30	38	118

Primzahl 137. Primitive Wurzeln 3, 5, 6, 12, 13, 20, 21, 23, 24, 26, 27, 29, 31, 33, 35, 40, 42, 43, 45, 46, 47, 48, 51, 52, 53, 54, 55, 57, 58, 62, 66, 67, 70, 71, 75, 79, 80, 82, 83, 84, 85, 86, 89, 90, 91, 92, 94, 95, 97, 102, 104, 106, 108, 110, 111, 113, 114, 116, 117, 124, 125, 131, 132, 134. *Basis 12.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	130	13	124	23	7	2	118	26
1	17	90	1	53	132	36	112	86	20	54
2	11	15	84	129	131	46	47	39	126	95
3	30	133	106	103	80	25	14	102	48	66
4	5	51	9	37	78	49	123	111	125	4
5	40	99	41	71	33	113	120	67	89	128
6	24	110	127	28	100	76	97	87	74	6
7	19	29	8	32	96	59	42	92	60	21
8	135	52	45	101	3	109	31	108	72	57
9	43	55	117	10	105	77	119	73	134	116
10	34	82	93	12	35	38	65	98	27	58
11	107	115	114	63	61	16	83	79	122	88
12	18	44	104	64	121	69	22	85	94	50
13	70	75	91	56	81	62	68			

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	12	7	84	49	40	69	6	72	42
1	93	20	103	3	36	21	115	10	120	70
2	18	79	126	5	60	35	9	108	63	71
3	30	86	73	54	100	104	15	43	105	27
4	50	52	76	90	121	82	25	26	38	45
5	129	41	81	13	19	91	133	89	109	75
6	78	114	135	113	123	106	39	57	136	125
7	130	53	88	97	68	131	65	95	44	117
8	34	134	101	116	22	127	17	67	119	58
9	11	132	77	102	128	29	74	66	107	51
10	64	83	37	33	122	94	32	110	87	85
11	61	47	16	55	112	111	99	92	8	96
12	56	124	118	46	4	48	28	62	59	23
13	2	24	14	31	98	80				

Primzahl 139. Primitive Wurzeln 2, 3, 12, 15, 17, 18, 19, 21, 22, 26, 32, 40, 50, 53, 56, 58, 61, 68, 70, 72, 73, 85, 88, 90, 92, 93, 98, 101, 102, 104, 108, 109, 110, 111, 114, 115, 119, 123, 126, 128, 130, 132, 134, 135. *Basis 92.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	119	49	100	22	30	16	81	98
1	3	74	11	26	135	71	62	37	79	83
2	122	65	55	39	130	44	7	9	116	8
3	52	40	43	123	18	38	60	136	64	75
4	103	82	46	23	36	120	20	70	111	32
5	25	86	126	73	128	96	97	132	127	15
6	33	125	21	114	24	48	104	110	137	88
7	19	68	41	35	117	93	45	90	56	102
8	84	58	63	28	27	59	4	57	17	94
9	101	42	1	89	51	105	92	115	13	34
10	6	133	67	129	107	87	54	112	109	121
11	77	47	78	76	113	61	108	124	134	53
12	14	10	106	131	2	66	95	80	5	72
13	29	12	85	99	91	31	118	50	69	

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	92	124	10	86	128	100	26	29	27
1	121	12	131	98	120	59	7	88	34	70
2	46	62	5	43	64	50	13	84	83	130
3	6	135	49	60	99	73	44	17	35	23
4	31	72	91	32	25	76	42	111	65	3
5	137	94	30	119	106	22	78	87	81	85
6	36	115	16	82	38	21	125	102	71	138
7	47	15	129	53	11	39	113	110	112	18
8	127	8	41	19	80	132	51	105	69	93
9	77	134	96	75	89	126	55	56	9	133
10	4	90	79	40	66	95	122	104	116	108
11	67	48	107	114	63	97	28	74	136	2
12	45	109	20	33	117	61	52	58	54	103
13	24	123	57	101	118	14	37	68		

Primzahl 149. Primitive Wurzeln 2, 3, 8, 10, 11, 12, 13, 14, 15, 18, 21, 23, 27, 32, 34, 38, 40, 41, 43, 48, 50, 51, 52, 55, 56, 57, 58, 59, 60, 62, 65, 66, 70, 71, 72, 74, 75, 77, 78, 79, 83, 84, 87, 89, 90, 91, 92, 93, 94, 97, 98, 99, 101, 106, 108, 109, 111, 115, 117, 122, 126, 128, 131, 134, 135, 136, 137, 138, 139, 141, 146, 147.

Basis 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	117	115	86	32	84	38	55	82
1	1	25	53	133	7	147	24	4	51	60
2	118	5	142	15	22	64	102	49	124	128
3	116	52	141	140	121	70	20	136	29	100
4	87	61	122	77	111	114	132	14	139	76
5	33	119	71	34	18	57	93	27	97	9
6	85	6	21	120	110	17	109	104	90	130
7	39	143	137	72	105	31	146	63	69	113
8	56	16	30	35	91	36	46	95	80	11
9	83	23	101	19	131	92	108	145	45	107
10	2	65	88	58	40	37	3	48	135	13
11	26	103	62	94	144	47	66	67	126	42
12	54	50	123	28	138	96	89	68	79	44
13	134	125	78	98	73	81	59	127	99	75
14	8	129	112	10	106	12	41	43	74	

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	10	100	106	17	21	61	14	140	59
1	143	89	145	109	47	23	81	65	54	93
2	36	62	24	91	16	11	110	57	123	38
3	82	75	5	50	53	83	85	105	7	70
4	104	146	119	147	129	98	86	115	107	27
5	121	18	31	12	120	8	80	55	103	136
6	19	41	112	77	25	101	116	117	127	78
7	35	52	73	134	148	139	49	43	132	128
8	88	135	9	90	6	60	4	40	102	126
9	68	84	95	56	113	87	125	58	133	138
10	39	92	26	111	67	74	144	99	96	66
11	64	44	142	79	45	3	30	2	20	51
12	63	34	42	122	28	131	118	137	29	141
13	69	94	46	13	130	108	37	72	124	48
14	33	32	22	71	114	97	76	15		

Primzahl 151. Primitive Wurzeln 6, 7, 12, 13, 14, 15, 30, 35, 48, 51, 52, 54, 56, 61, 63, 71, 77, 82, 89, 93, 96, 102, 104, 106, 108, 109, 111, 112, 114, 115, 117, 120, 126, 129, 130, 133, 134, 140, 141, 146. *Basis 114.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	70	141	140	82	61	37	60	132
1	2	34	131	101	107	73	130	88	52	90
2	72	28	104	115	51	14	21	123	27	54
3	143	58	50	25	8	119	122	76	10	92
4	142	111	98	38	24	64	35	86	121	74
5	84	79	91	69	43	116	97	81	124	30
6	63	59	128	19	120	33	95	93	78	106
7	39	137	42	87	146	5	80	71	12	117
8	62	114	31	3	18	20	108	45	94	53
9	134	138	105	49	6	22	41	118	144	16
10	4	9	149	46	11	110	139	99	113	23
11	36	67	17	85	1	47	44	83	100	125
12	133	68	129	102	48	96	89	126	40	29
13	103	147	15	127	13	55	148	32	26	56
14	109	77	57	135	112	136	7	65	66	145
15	75									

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	114	10	83	100	75	94	146	34	101
1	38	104	78	134	25	132	99	112	84	63
2	85	26	95	109	44	33	138	28	21	129
3	59	82	137	65	11	46	110	7	43	70
4	128	96	72	54	116	87	103	115	124	93
5	32	24	18	89	29	135	139	142	31	61
6	8	6	80	60	45	147	148	111	121	53
7	2	77	20	15	49	150	37	141	68	51
8	76	57	5	117	50	113	47	73	17	126
9	19	52	39	67	88	66	125	56	42	107
10	118	13	123	130	22	92	69	14	86	140
11	105	41	144	108	81	23	55	79	97	35
12	64	48	36	27	58	119	127	133	62	122
13	16	12	9	120	90	143	145	71	91	106
14	4	3	40	30	98	149	74	131	136	102

Primzahl 157. Primitive Wurzeln 5, 6, 15, 18, 20, 21, 24, 26, 34, 38, 43, 53, 55, 60, 61, 62, 63, 66, 69, 70, 72, 73, 74, 77, 80, 83, 84, 85, 87, 88, 91, 94, 95, 96, 97, 102, 104, 114, 119, 123, 131, 133, 136, 137, 139, 142, 151, 152. *Basis 139.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	147	122	138	11	113	57	129	88
1	2	152	104	130	48	133	120	128	79	116
2	149	23	143	81	95	22	121	54	39	15
3	124	58	111	118	119	68	70	28	107	96
4	140	75	14	151	134	99	72	76	86	114
5	13	94	112	25	45	7	30	82	6	27
6	115	155	49	145	102	141	109	12	110	47
7	59	64	61	83	19	144	98	53	87	9
8	131	20	66	97	5	139	142	137	125	32
9	90	31	63	24	67	127	77	37	105	84
10	4	108	85	123	103	34	16	91	36	8
11	154	150	21	56	73	92	153	62	18	29
12	106	148	146	41	40	33	136	46	93	117
13	132	43	100	17	3	65	101	71	38	1
14	50	42	55	126	52	26	74	80	10	51
15	135	35	89	60	44	69	78			

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	139	10	134	100	84	58	55	109	79
1	148	5	67	50	42	29	106	133	118	74
2	81	112	25	21	93	53	145	59	37	119
3	56	91	89	125	105	151	108	97	138	28
4	124	123	141	131	154	54	127	69	14	62
5	140	149	144	77	27	142	113	7	31	70
6	153	72	117	92	71	135	82	94	35	155
7	36	137	46	114	146	41	47	96	156	18
8	147	23	57	73	99	102	48	78	9	152
9	90	107	115	128	51	24	39	83	76	45
10	132	136	64	104	12	98	120	38	101	66
11	68	32	52	6	49	60	19	129	33	34
12	16	26	3	103	30	88	143	95	17	8
13	13	80	130	15	44	150	126	87	4	85
14	40	65	86	22	75	63	122	2	121	20
15	111	43	11	116	110	61				

Primzahl 163. Primitive Wurzeln 2, 3, 7, 11, 12, 18, 19, 20, 29, 32, 42, 44, 45, 50, 52, 63, 66, 67, 68, 70, 72, 73, 75, 76, 79, 80, 82, 89, 92, 94, 101, 103, 106, 107, 108, 109, 112, 114, 116, 117, 120, 122, 124, 128, 129, 130, 137, 139, 147, 148, 149, 153, 154, 159. *Basis 70.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	71	43	142	93	114	161	51	86
1	2	97	23	57	70	136	122	159	157	127
2	73	42	6	153	94	24	128	129	141	145
3	45	39	31	140	68	92	66	75	36	100
4	144	20	113	106	77	17	62	44	3	160
5	95	40	37	18	38	28	50	8	54	27
6	116	30	110	85	102	150	49	155	139	34
7	1	52	137	7	146	67	107	96	9	103
8	53	10	91	134	22	90	15	26	148	65
9	88	56	133	82	115	58	74	130	69	21
10	4	29	111	35	108	135	89	131	109	119
11	99	118	121	14	79	84	125	143	98	158
12	25	32	101	63	19	117	156	147	11	149
13	59	112	120	126	64	60	48	47	105	13
14	72	87	123	154	46	76	78	41	55	151
15	138	104	16	83	5	132	80	33	12	61
16	124	152	81							

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	70	10	48	100	154	22	73	57	78
1	81	128	158	139	113	86	152	45	53	124
2	41	99	84	12	25	120	87	59	55	101
3	61	32	121	157	69	103	38	52	54	31
4	51	147	21	3	47	30	144	137	136	66
5	56	8	71	80	58	148	91	13	95	130
6	135	159	46	123	134	89	36	75	34	98
7	14	2	140	20	96	37	145	44	146	114
8	156	162	93	153	115	63	9	141	90	106
9	85	82	35	5	24	50	77	11	118	110
10	39	122	64	79	151	138	43	76	104	108
11	62	102	131	42	6	94	60	125	111	109
12	132	112	16	142	160	116	133	19	26	27
13	97	107	155	92	83	105	15	72	150	68
14	33	28	4	117	40	29	74	127	88	129
15	65	149	161	23	143	67	126	18	119	17
16	49	7								

Primzahl 167. Primitive Wurzeln 5, 10, 13, 15, 17, 20, 23, 26, 30, 34, 35, 37, 39, 40, 41, 43, 45, 46, 51, 52, 53, 55, 59, 60, 67, 68, 69, 70, 71, 73, 74, 78, 79, 80, 82, 83, 86, 90, 91, 92, 95, 101, 102, 103, 104, 105, 106, 109, 110, 111, 113, 117, 118, 119, 120, 123, 125, 129, 131, 134, 135, 136, 138, 139, 140, 142, 143, 145, 146, 148, 149, 151, 153, 155, 156, 158, 159, 160, 161, 163, 164, 165. *Basis 10.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	86	144	6	81	64	96	92	122
1	1	110	150	43	16	59	12	143	42	50
2	87	74	30	51	70	162	129	100	102	32
3	145	152	98	88	63	11	128	127	136	21
4	7	55	160	75	116	37	137	68	156	26
5	82	121	49	31	20	25	22	28	118	23
6	65	34	72	52	18	124	8	85	149	29
7	97	159	48	71	47	140	56	40	107	119
8	93	78	141	163	80	58	161	10	36	24
9	123	139	57	130	154	131	76	14	112	66
10	2	91	41	101	135	155	117	148	106	35
11	111	105	108	103	114	132	38	165	109	73
12	151	54	120	33	158	77	138	90	104	53
13	44	45	94	146	5	15	69	62	115	19
14	17	46	79	153	134	113	157	4	133	125
15	60	95	142	99	126	67	27	84	39	9
16	13	147	164	89	61	3	83			

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	10	100	165	147	134	4	40	66	159
1	87	35	16	160	97	135	14	140	64	139
2	54	39	56	59	89	55	49	156	57	69
3	22	53	29	123	61	109	88	45	116	158
4	77	102	18	13	130	131	141	74	72	52
5	19	23	63	129	121	41	76	92	85	15
6	150	164	137	34	6	60	99	155	47	136
7	24	73	62	119	21	43	96	125	81	142
8	84	5	50	166	157	67	2	20	33	163
9	127	101	8	80	132	151	7	70	32	153
10	27	103	28	113	128	111	108	78	112	118
11	11	110	98	145	114	138	44	106	58	79
12	122	51	9	90	65	149	154	37	36	26
13	93	95	115	148	144	104	38	46	126	91
14	75	82	152	17	3	30	133	161	107	68
15	12	120	31	143	94	105	48	146	124	71
16	42	86	25	83	162	117				

Primzahl 173. Primitive Wurzeln 2, 3, 5, 7, 8, 11, 12, 17, 18, 19, 20, 26, 27, 28, 30, 32, 39, 42, 44, 45, 46, 48, 50, 53, 58, 59, 61, 62, 63, 65, 66, 68, 69, 70, 71, 72, 74, 75, 76, 79, 82, 86, 87, 91, 94, 97, 98, 99, 101, 102, 103, 104, 105, 107, 108, 110, 111, 112, 114, 115, 120, 123, 125, 127, 128, 129, 131, 134, 141, 143, 145, 146, 147, 153, 154, 155, 156, 161, 162, 165, 166, 168, 170, 171. *Basis 91.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	13	7	26	163	20	31	39	14
1	4	127	33	142	44	170	52	89	27	85
2	17	38	140	88	46	154	155	21	57	152
3	11	122	65	134	102	22	40	42	98	149
4	30	74	51	60	153	5	101	144	59	62
5	167	96	168	123	34	118	70	92	165	19
6	24	169	135	45	78	133	147	50	115	95
7	35	23	53	94	55	161	111	158	162	71
8	43	28	87	104	64	80	73	159	166	150
9	18	1	114	129	157	76	72	25	75	141
10	8	139	109	121	9	29	136	61	47	164
11	131	49	83	110	105	79	6	156	32	120
12	37	82	10	81	148	145	58	15	91	67
13	146	137	160	116	63	12	128	126	108	16
14	48	151	36	97	66	143	107	69	68	132
15	2	54	124	103	171	113	3	138	84	130
16	56	119	41	90	100	125	117	106	77	112
17	93	99	86							

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	91	150	156	10	45	116	3	100	104
1	122	30	135	2	9	127	139	20	90	59
2	6	27	35	71	60	97	4	18	81	105
3	40	7	118	12	54	70	142	120	21	8
4	36	162	37	80	14	63	24	108	140	111
5	67	42	16	72	151	74	160	28	126	48
6	43	107	49	134	84	32	144	129	148	147
7	56	79	96	86	41	98	95	168	64	115
8	85	123	121	112	158	19	172	82	23	17
9	163	128	57	170	73	69	51	143	38	171
10	164	46	34	153	83	114	167	146	138	102
11	113	76	169	155	92	68	133	166	55	161
12	119	103	31	53	152	165	137	11	136	93
13	159	110	149	65	33	62	106	131	157	101
14	22	99	13	145	47	125	130	66	124	39
15	89	141	29	44	25	26	117	94	77	87
16	132	75	78	5	109	58	88	50	52	61
17	15	154								

Primzahl 179. Primitive Wurzeln 2, 6, 7, 8, 10, 11, 18, 21, 23, 24, 26, 28, 30, 32, 33, 34, 35, 37, 38, 40, 41, 44, 50, 53, 54, 55, 58, 62, 63, 69, 71, 72, 73, 78, 79, 84, 86, 90, 91, 92, 94, 96, 97, 98, 99, 102, 103, 104, 105, 109, 111, 112, 113, 114, 115, 118, 119, 120, 122, 123, 127, 128, 130, 131, 132, 133, 134, 136, 137, 140, 143, 148, 150, 152, 154, 157, 159, 160, 162, 163, 164, 165, 166, 167, 170, 174, 175, 176.

Basis 10.

I.

N	0	1	2	3	4	5	6	7	8	9
		0	73	52	146	106	125	23	41	104
1	1	27	20	134	96	158	114	14	177	26
2	74	75	100	65	93	34	29	156	169	70
3	53	76	9	79	87	129	72	19	99	8
4	147	101	148	144	173	32	138	136	166	46
5	107	66	102	111	51	133	64	78	143	110
6	126	94	149	127	82	62	152	48	160	117
7	24	35	145	95	92	86	172	50	81	91
8	42	30	174	150	43	120	39	122	68	16
9	105	157	33	128	31	132	61	85	119	131
10	2	170	139	83	175	3	6	56	124	113
11	28	71	137	63	151	171	38	60	5	37
12	21	54	167	153	44	140	22	13	155	18
13	135	77	47	49	121	84	55	59	12	58
14	97	10	108	161	40	176	168	98	165	142
15	159	80	67	118	123	4	154	11	164	163
16	115	88	103	25	69	7	45	109	116	90
17	15	130	112	36	17	57	141	162	89	

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	10	100	105	155	118	106	165	39	32
1	141	157	138	127	17	170	89	174	129	37
2	12	120	126	7	70	163	19	11	110	26
3	81	94	45	92	25	71	173	119	116	86
4	144	8	80	84	124	166	49	132	67	133
5	77	54	3	30	121	136	107	175	139	137
6	117	96	65	113	56	23	51	152	88	164
7	29	111	36	2	20	21	31	131	57	33
8	151	78	64	103	135	97	75	34	161	178
9	169	79	74	24	61	73	14	140	147	38
10	22	41	52	162	9	90	5	50	142	167
11	59	53	172	109	16	160	168	69	153	98
12	85	134	87	154	108	6	60	63	93	35
13	171	99	95	55	13	130	47	112	46	102
14	125	176	149	58	43	72	4	40	42	62
15	83	114	66	123	156	128	27	91	15	150
16	68	143	177	159	158	148	48	122	146	28
17	101	115	76	44	82	104	145	18		

Primzahl 181. Primitive Wurzeln 2, 10, 18, 21, 23, 24, 28, 41, 47, 50, 53, 54, 57, 58, 63, 66, 69, 76, 77, 78, 83, 84, 85, 90, 91, 96, 97, 98, 103, 104, 105, 112, 115, 118, 123, 124, 127, 128, 131, 134, 140, 153, 157, 158, 160, 163, 171, 179.

Basis 10.

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	133	68	86	48	21	15	39	136
1	1	146	154	32	148	116	172	55	89	135
2	134	83	99	29	107	96	165	24	101	84
3	69	27	125	34	8	63	42	38	88	100
4	87	59	36	140	52	4	162	109	60	30
5	49	123	118	121	157	14	54	23	37	108
6	22	65	160	151	78	80	167	66	141	97
7	16	57	175	20	171	164	41	161	53	166
8	40	92	12	73	169	103	93	152	5	25
9	137	47	115	95	62	3	13	79	163	102
10	2	130	76	143	71	131	74	81	110	85
11	147	106	7	51	156	77	170	168	61	70
12	155	112	18	127	113	144	104	67	31	28
13	33	139	120	150	19	72	94	142	50	126
14	149	177	10	178	128	132	153	98	124	35
15	117	159	174	11	114	75	6	17	119	9
16	173	44	45	179	145	82	26	58	122	64
17	56	91	46	129	105	111	138	176	158	43
18	90									

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	10	100	95	45	88	156	112	34	159
1	142	153	82	96	55	7	70	157	122	134
2	73	6	60	57	27	89	166	31	129	23
3	49	128	13	130	33	149	42	58	37	8
4	80	76	36	179	161	162	172	91	5	50
5	138	113	44	78	56	17	170	71	167	41
6	48	118	94	35	169	61	67	127	3	30
7	119	104	135	83	106	155	102	115	64	97
8	65	107	165	21	29	109	4	40	38	18
9	180	171	81	86	136	93	25	69	147	22
10	39	28	99	85	126	174	111	24	59	47
11	108	175	121	124	154	92	15	150	52	158
12	132	53	168	51	148	32	139	123	144	173
13	101	105	145	2	20	19	9	90	176	131
14	43	68	137	103	125	164	11	110	14	140
15	133	63	87	146	12	120	114	54	178	151
16	62	77	46	98	75	26	79	66	117	84
17	116	74	16	160	152	72	177	141	143	163

Primzahl 191. Primitive Wurzeln 19, 21, 22, 28, 29, 33, 35, 42, 44, 47, 53, 56, 57, 58, 61, 62, 63, 71, 73, 74, 76, 83, 87, 88, 89, 91, 93, 94, 95, 99, 101, 105, 106, 110, 111, 112, 113, 114, 116, 119, 123, 124, 126, 127, 131, 132, 137, 140, 141, 143, 145, 146, 148, 151, 157, 164, 165, 167, 168, 171, 173, 174, 176, 178, 179, 181, 182, 183, 187, 188, 189. *Basis 157.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	102	148	14	90	60	133	116	106
1	2	115	162	156	45	48	28	184	18	93
2	104	91	27	112	74	180	68	64	147	29
3	150	125	130	73	96	33	120	65	5	114
4	16	145	3	174	129	6	24	39	176	76
5	92	142	170	77	166	15	59	51	131	182
6	62	63	37	49	42	56	175	44	8	70
7	135	69	32	189	167	138	107	58	26	66
8	118	22	57	173	105	84	86	177	41	149
9	108	99	126	83	141	183	88	46	178	31
10	4	13	54	136	82	181	179	10	78	152
11	117	23	161	121	153	12	43	72	94	127
12	164	40	165	103	139	80	151	137	144	132
13	158	157	87	36	146	154	110	71	172	75
14	47	187	171	81	134	119	101	34	79	98
15	50	111	19	100	160	25	128	1	168	35
16	30	55	124	52	159	163	85	169	17	122
17	186	9	188	113	89	123	143	140	61	67
18	20	97	11	21	38	155	185	109	53	7
19	95									

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	157	10	42	100	38	45	189	68	171
1	107	182	115	101	4	55	40	168	18	152
2	180	183	81	111	46	155	78	22	16	29
3	160	99	72	35	147	159	133	62	184	47
4	121	88	64	116	67	14	97	140	15	63
5	150	57	163	188	102	161	65	82	77	56
6	6	178	60	61	27	37	79	179	26	71
7	69	137	117	33	24	139	49	53	108	148
8	125	143	104	93	85	166	86	132	96	174
9	5	21	50	19	118	190	34	181	149	91
10	153	146	2	123	20	84	9	76	90	187
11	136	151	23	173	39	11	8	110	80	145
12	36	113	169	175	162	31	92	119	156	44
13	32	58	129	7	144	70	103	127	75	124
14	177	94	51	176	128	41	134	28	3	89
15	30	126	109	114	135	185	13	131	130	164
16	154	112	12	165	120	122	54	74	158	167
17	52	142	138	83	43	66	48	87	98	106
18	25	105	59	95	17	186	170	141	172	73

Primzahl 193. Primitive Wurzeln 5, 10, 15, 17, 19, 22, 26, 30, 34, 37, 38, 40, 41, 44, 45, 47, 51, 52, 53, 57, 58, 61, 66, 70, 73, 77, 78, 79, 80, 82, 90, 91, 102, 103, 111, 113, 114, 115, 116, 120, 123, 127, 132, 135, 136, 140, 141, 142, 146, 148, 149, 152, 153, 155, 156, 159, 163, 167, 171, 174, 176, 178, 183, 188. *Basis 10.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	182	156	172	11	146	184	162	120
1	1	93	136	15	174	167	152	149	110	59
2	183	148	83	54	126	22	5	84	164	9
3	157	134	142	57	139	3	100	55	49	171
4	173	125	138	72	73	131	44	127	116	176
5	12	113	187	79	74	104	154	23	191	92
6	147	133	124	112	132	26	47	6	129	18
7	185	27	90	41	45	178	39	85	161	109
8	163	48	115	190	128	160	62	165	63	81
9	121	7	34	98	117	70	106	10	166	21
10	2	130	103	25	177	159	69	158	64	32
11	94	19	144	67	13	65	181	135	82	141
12	137	186	123	89	114	33	102	143	122	36
13	16	28	37	51	188	95	119	58	8	170
14	175	91	17	108	80	20	31	140	35	169
15	168	42	29	77	75	145	151	4	99	43
16	153	46	38	61	105	68	180	101	118	30
17	150	179	52	87	155	14	53	56	71	78
18	111	40	189	97	24	66	88	50	107	76
19	60	86	96							

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	10	100	35	157	26	67	91	138	29
1	97	5	50	114	175	13	130	142	69	111
2	145	99	25	57	184	103	65	71	131	152
3	169	146	109	125	92	148	129	132	162	76
4	181	73	151	159	46	74	161	66	81	38
5	187	133	172	176	23	37	177	33	137	19
6	190	163	86	88	108	115	185	113	165	106
7	95	178	43	44	54	154	189	153	179	53
8	144	89	118	22	27	77	191	173	186	123
9	72	141	59	11	110	135	192	183	93	158
10	36	167	126	102	55	164	96	188	143	79
11	18	180	63	51	124	82	48	94	168	136
12	9	90	128	122	62	41	24	47	84	68
13	101	45	64	61	31	117	12	120	42	34
14	147	119	32	127	112	155	6	60	21	17
15	170	156	16	160	56	174	3	30	107	105
16	85	78	8	80	28	87	98	15	150	149
17	139	39	4	40	14	140	49	104	75	171
18	166	116	2	20	7	70	121	52	134	182
19	83	58								

Primzahl 197. Primitive Wurzeln 2, 3, 5, 8, 11, 12, 13, 17, 18, 21, 27, 30, 31, 32, 35, 38, 44, 45, 46, 48, 50, 52, 56, 57, 58, 66, 67, 71, 72, 73, 74, 75, 78, 79, 80, 82, 86, 89, 91, 94, 95, 98, 99, 102, 103, 106, 108, 111, 115, 117, 118, 119, 122, 123, 124, 125, 126, 130, 131, 139, 140, 141, 145, 147, 149, 151, 152, 153, 159, 162, 165, 166, 167, 170, 176, 179, 180, 184, 185, 186, 189, 192, 194, 195. *Basis 73.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	61	65	122	137	126	86	183	130
1	2	5	187	153	147	6	48	95	191	182
2	63	151	66	68	52	78	18	195	12	40
3	67	173	109	70	156	27	56	148	47	22
4	124	46	16	54	127	71	129	106	113	172
5	139	160	79	80	60	142	73	51	101	96
6	128	180	38	20	170	94	131	57	21	133
7	88	179	117	1	13	143	108	91	83	59
8	185	64	107	14	77	36	115	105	188	23
9	132	43	190	42	167	123	174	102	37	135
10	4	76	25	69	140	92	141	34	121	90
11	7	17	134	175	112	9	162	87	157	181
12	189	10	45	111	99	19	81	186	35	119
13	155	33	192	72	118	136	82	30	194	3
14	149	171	44	158	178	177	62	41	74	15
15	8	31	169	29	152	114	144	26	120	145
16	50	154	125	58	168	11	75	165	138	110
17	97	116	176	150	166	164	53	161	84	93
18	193	146	104	49	55	89	103	100	32	85
19	184	28	39	24	163	159	98			

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	73	10	139	100	11	15	110	150	115
1	121	165	28	74	83	149	42	111	26	125
2	63	68	39	89	193	102	157	35	191	153
3	137	151	188	131	107	128	85	98	62	192
4	29	147	93	91	142	122	41	38	16	183
5	160	57	24	176	43	184	36	67	163	79
6	54	2	146	20	81	3	22	30	23	103
7	33	45	133	56	148	166	101	84	25	52
8	53	126	136	78	178	189	7	117	70	185
9	109	77	105	179	65	17	59	170	196	124
10	187	58	97	186	182	87	47	82	76	32
11	169	123	114	48	155	86	171	72	134	129
12	158	108	4	95	40	162	6	44	60	46
13	9	66	90	69	112	99	135	5	168	50
14	104	106	55	75	156	159	181	14	37	140
15	173	21	154	13	161	130	34	118	143	195
16	51	177	116	194	175	167	174	94	164	152
17	64	141	49	31	96	113	172	145	144	71
18	61	119	19	8	190	80	127	12	88	120
19	92	18	132	180	138	27				

Primzahl 199. Primitive Wurzeln 3, 6, 15, 22, 30, 34, 38, 39, 41, 44, 48, 54, 68, 69, 71, 73, 75, 77, 84, 87, 95, 97, 99, 105, 108, 110, 113, 118, 119, 120, 127, 129, 133, 134, 142, 143, 146, 148, 149, 150, 152, 153, 154, 163, 164, 166, 167, 168, 170, 173, 176, 179, 183, 185, 186, 189, 190, 192, 195, 197. *Basis 127.*

I.

N.	0	1	2	3	4	5	6	7	8	9
		0	194	155	190	6	151	32	186	112
1	2	189	147	128	28	161	182	57	108	11
2	196	187	185	74	143	12	124	69	24	158
3	157	76	178	146	53	38	104	121	7	85
4	192	145	183	176	181	118	70	98	139	64
5	8	14	120	136	65	195	20	166	154	129
6	153	126	72	144	174	134	142	39	49	31
7	34	71	100	41	117	167	3	23	81	50
8	188	26	141	51	179	63	172	115	177	92
9	114	160	66	33	94	17	135	109	60	103
10	4	159	10	36	116	193	132	165	61	15
11	191	78	16	73	162	80	150	42	125	89
12	149	180	122	102	68	18	140	1	170	133
13	130	148	138	43	35	75	45	171	27	54
14	30	55	67	119	96	164	37	21	113	107
15	163	40	197	169	19	82	77	84	46	93
16	184	106	22	5	137	152	47	79	175	58
17	59	123	168	25	111	44	173	86	88	97
18	110	9	156	83	62	127	29	48	90	101
19	13	87	131	52	105	91	56	95	99	

N.

I.	0	1	2	3	4	5	6	7	8	9
	1	127	10	76	100	163	5	38	50	181
1	102	19	25	190	51	109	112	95	125	154
2	56	147	162	77	28	173	81	138	14	186
3	140	69	7	93	70	134	103	146	35	67
4	151	73	117	133	175	136	158	166	187	68
5	79	83	193	24	139	141	196	17	169	170
6	98	108	184	85	49	54	92	142	124	27
7	46	71	62	113	23	135	31	156	111	167
8	115	78	155	183	157	39	177	191	178	119
9	188	195	89	159	94	197	144	179	47	198
10	72	189	123	99	36	194	161	149	18	97
11	180	174	9	148	90	87	104	74	45	143
12	52	37	122	171	26	118	61	185	13	59
13	130	192	106	129	65	96	53	164	132	48
14	126	82	66	24	63	41	33	12	131	120
15	116	6	165	60	58	3	182	30	29	101
16	91	15	114	150	145	107	57	75	172	153
17	128	137	86	176	64	168	43	88	32	84
18	121	44	16	42	160	22	8	21	80	11
19	4	110	40	105	2	55	20	152		

Lineare Theiler

der quadratischen Form $x^2 + ay^2$ für alle Werthe von a von 1 bis 101.

Form	Lineare Theiler
$x^2 + y^2$	$4z +$ 1.
$x^2 + 2y^2$	$8z +$ 1, 3.
$x^2 + 3y^2$	$12z +$ 1, 7.
$x^2 + 5y^2$	$20z +$ 1, 3, 7, 9.
$x^2 + 6y^2$	$24z +$ 1, 5, 7, 11.
$x^2 + 7y^2$	$28z +$ 1, 9, 11, 15, 23, 25.
$x^2 + 10y^2$	$40z +$ 1, 7, 9, 11, 13, 19, 23, 37.
$x^2 + 11y^2$	$44z +$ 1, 3, 5, 9, 15, 23, 25, 27, 31, 37.
$x^2 + 13y^2$	$52z +$ 1, 7, 9, 11, 15, 17, 19, 25, 29, 31, 47, 49.
$x^2 + 14y^2$	$56z +$ 1, 3, 5, 9, 13, 15, 19, 23, 25, 27, 39, 45.
$x^2 + 15y^2$	$60z +$ 1, 17, 19, 23, 31, 47, 49, 53.
$x^2 + 17y^2$	$68z +$ 1, 3, 7, 9, 11, 13, 21, 23, 25, 27, 31, 33, 39, 49, 53, 63.
$x^2 + 19y^2$	$76z +$ 1, 5, 7, 9, 11, 17, 23, 25, 35, 39, 43, 45, 47, 49, 55, 61, 63, 73.
$x^2 + 21y^2$	$84z +$ 1, 5, 11, 17, 19, 23, 25, 31, 37, 41, 55, 71.
$x^2 + 22y^2$	$88z +$ 1, 9, 13, 15, 19, 21, 23, 25, 29, 31, 35, 43, 47, 49, 51, 61, 71; 81, 83, 85.
$x^2 + 23y^2$	$92z +$ 1, 3, 9, 13, 25, 27, 29, 31, 35, 39, 41, 47, 49, 55, 59, 71, 73; 75, 77, 81, 85, 87.
$x^2 + 26y^2$	$104z +$ 1, 3, 5, 7, 9, 15, 17, 21, 25, 27, 31, 35, 37, 43, 45, 47, 49. 51; 63, 71, 75, 81, 85, 93.
$x^2 + 29y^2$	$116z +$ 1, 3, 5, 9. 11, 13, 15, 19, 25, 27, 31, 33, 39, 43, 45, 47, 49, 53, 55, 57, 65, 75, 79, 81, 93, 95, 99, 109.
$x^2 + 30y^2$	$120z +$ 1, 11, 13, 17, 23, 29, 31, 37, 43, 47, 49, 59. 67, 79, 101, 113.
$x^2 + 31y^2$	$124z +$ 1, 5, 7, 9, 19, 25, 33, 35, 39, 41, 45, 47, 49, 51, 59, 63, 67, 69, 71, 81, 87, 95, 97, 101, 103, 107, 109, 111, 113, 121.
$x^2 + 33y^2$	$132z +$ 1, 7, 17, 19, 23, 25, 29, 37, 41, 43, 47, 49, 59, 65, 71, 79, 97, 101, 119, 127.
$x^2 + 34y^2$	$136z +$ 1, 5, 7, 9, 19, 23, 25, 29, 31, 33, 35, 37, 39, 43, 45, 49, 59, 61, 63, 67, 71, 79, 81, 83, 89, 95, 109, 115, 121, 123, 125, 133.
$x^2 + 35y^2$	$140z +$ 1, 3, 9, 11, 13, 17, 27, 29, 33, 39, 47, 51, 71, 73, 79, 81, 83, 87, 97, 99, 103, 109, 117, 121.

$x^2 + 37y^2$	$148z +$ 1, 9, 15, 19, 21, 23, 25, 31, 33, 35, 39, 41, 43, 49, 51, 53, 55, 59, 65, 73, 77, 79, 81, 85, 87, 91, 101, 103, 119, 121, 131, 135, 137, 141, 143, 145.
$x^2 + 38y^2$	$152z +$ 1, 3, 7, 9, 13, 17, 21, 23, 25, 27, 29, 37, 39, 47, 49, 51, 53, 55, 59, 63, 67, 69, 73, 75, 81, 87, 91, 107, 109, 111, 117, 119, 121, 137, 141, 147.
$x^2 + 39y^2$	$156z +$ 1, 5, 11, 25, 41, 43, 47, 49, 55, 59, 61, 71, 79, 83, 89, 103, 119, 121, 125, 127, 133, 137, 139, 149.
$x^2 + 41y^2$	$164z +$ 1, 3, 5, 7, 9, 11, 15, 19, 21, 25, 27, 33, 35, 37, 45, 47, 49, 55, 57, 61, 63, 67, 71, 73, 75, 77, 79, 81, 95, 99, 105, 111, 113, 121, 125, 133, 135, 141, 147, 151.
$x^2 + 42y^2$	$168z +$ 1, 13, 17, 23, 25, 29, 31, 41, 43, 53, 55, 59, 61, 67, 71, 83, 89, 95, 103, 121, 131, 149, 159, 163.
$x^2 + 43y^2$	$172z +$ 1, 9, 11, 13, 15, 17, 21, 23, 25, 31, 35, 41, 47, 49, 53, 57, 59, 67, 79, 81, 83, 87, 95, 97, 99, 101, 103, 107, 109, 111, 117, 121, 127, 133, 135, 139, 143, 145, 153, 165, 167, 169.
$x^2 + 46y^2$	$184z +$ 1, 5, 9, 11, 19, 21, 25, 31, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 61, 67, 71, 73, 81, 83, 87, 91, 95, 99, 105, 107, 109, 119, 121, 125, 127, 149, 151, 155, 157, 167, 169, 171, 177, 181.
$x^2 + 47y^2$	$188z +$ 1, 3, 7, 9, 17, 21, 25, 27, 37, 49, 51, 53, 55, 59, 61, 63, 65, 71, 75, 79, 81, 83, 89, 95, 97, 101, 103, 111, 115, 119, 121, 131, 143, 145, 147, 149, 153, 155, 157, 159, 165, 169, 173, 175, 177, 183.
$x^2 + 51y^2$	$204z +$ 1, 5, 11, 13, 19, 23, 25, 29, 41, 43, 49, 55, 65, 67, 71, 95, 103, 107, 113, 115, 121, 125, 127, 131, 143, 145, 151, 157, 167, 169, 173, 197.
$x^2 + 53y^2$	$212z +$ 1, 3, 9, 13, 17, 19, 23, 25, 27, 29, 31, 35, 37, 39, 49, 51, 55, 57, 67, 69, 71, 75, 77, 79, 81, 83, 87, 89, 93, 97, 103, 105, 111, 113, 117, 121, 127, 139, 147, 149, 151, 153, 165, 167, 169, 171, 179, 191, 197, 201, 205, 207.
$x^2 + 55y^2$	$220z +$ 1, 7, 9, 13, 17, 31, 43, 49, 57, 59, 63, 69, 71, 73, 81, 83, 87, 89, 91, 107, 111, 117, 119, 123, 127, 141, 153, 159, 167, 169, 173, 179, 181, 183, 191, 193, 197, 199, 201, 217.
$x^2 + 57y^2$	$228z +$ 1, 11, 23, 25, 29, 31, 35, 41, 47, 49, 53, 61, 65, 67, 73, 79, 83, 85, 89, 91, 103, 113, 119, 121, 127, 131, 151, 157, 169, 173, 185, 191, 211, 215, 221, 223.
$x^2 + 58y^2$	$232z +$ 1, 9, 15, 21, 25, 31, 33, 35, 37, 39, 47, 49, 51, 55, 57, 59, 61, 65, 67, 69, 77, 79, 81, 83, 85, 91, 95, 101, 107, 115, 119, 121, 123, 127, 129, 133, 135, 139, 143, 157, 159, 161, 169, 179, 187, 189, 191, 205, 209, 213, 215, 219, 221, 225, 227, 229.
$x^2 + 59y^2$	$236z +$ 1, 3, 5, 7, 9, 15, 17, 19, 21, 25, 27, 29, 35, 41, 45, 49, 51, 53, 57, 63, 71, 75, 79, 81, 85, 87, 95, 105, 107, 119, 121, 123, 125, 127, 133, 135, 137, 139, 143, 145, 147, 153, 159, 163, 167, 169, 171, 175, 181, 189, 193, 197, 199, 203, 205, 213, 223, 225.

$x^2 + 61 y^2$	$244 z +$ 1, 5, 7, 9, 11, 13, 23, 25, 31, 35, 41, 43, 45, 49, 51, 55, 57, 59, 63, 65, 67, 71, 73, 77, 79, 81, 87, 91, 97, 99, 109, 111, 113, 115. 117, 121, 125, 137, 139, 141, 143, 149, 151, 155, 159, 161, 169, 175, 191, 197, 205, 207, 211, 217, 223, 225, 227, 229, 241.
$x^2 + 62 y^2$	$248 z +$ 1, 3, 7, 9, 11, 13, 21, 25, 27, 29, 33, 37, 39, 41, 43, 47, 49, 53, 61, 63, 71, 75, 77, 81, 83, 85, 87, 91, 95, 97, 99, 103, 111, 113, 115, 117, 121, 123, 129, 139, 141, 143, 147, 159, 169, 175, 179, 181, 183, 189, 191, 193, 197, 203, 213, 225, 229, 231, 233, 243.
$x^2 + 65 y^2$	$260 z +$ 1, 3, 9, 11, 19, 23, 27, 29, 31, 33, 37, 43, 49, 57, 59, 61, 69, 71, 73, 81, 87, 93, 97, 99, 101, 103, 107, 111, 119, 121, 127, 129, 137, 147, 151, 171, 177, 181, 183, 193, 197, 207, 209, 213, 219, 239, 243, 253.
$x^2 + 66 y^2$	$264 z +$ 1, 5, 7, 13, 17, 23, 25, 35, 41, 47, 49, 53, 61, 65, 67, 77, 79, 83. 85, 91, 97, 107, 109, 115, 119, 125, 127, 131, 151, 161, 163, 169, 175, 191, 205, 221, 227, 233, 235, 245.
$x^2 + 67 y^2$	$268 z +$ 1, 9, 15, 17, 19, 21, 23, 25, 29, 33, 35, 37, 39, 47, 49, 55, 59, 65, 71, 73, 77, 81, 83, 89, 91, 93, 103, 107, 121, 123, 127, 129, 131, 135, 143, 149, 151, 153, 155, 157, 159, 163, 167, 169, 171, 173, 181, 183, 189, 193, 199, 205, 207, 211, 215, 217, 223, 225, 227, 237, 241, 255, 257, 261, 263, 265.
$x^2 + 69 y^2$	$276 z +$ 1, 5, 7, 13, 17, 19, 25, 35, 43, 47, 49, 53, 59, 65, 67, 71, 73, 79, 85, 89, 91, 95, 103, 113, 119, 121, 125, 131, 133, 137, 149, 167, 169, 175, 179, 193, 199, 215, 221, 235, 239, 245, 247, 265.
$x^2 + 70 y^2$	$280 z +$ 1, 9, 17, 19, 33, 37, 39, 43, 47, 53, 59, 61, 67, 69, 71, 73, 79, 81, 87, 93, 97, 101, 103, 107, 121, 123, 131, 139, 143, 151, 153, 163, 167, 169, 171, 181, 191, 197, 223, 229, 233, 249, 251, 253, 257, 267, 269, 277.
$x^2 + 71 y^2$	$284 z +$ 1, 3, 5, 9, 15, 19, 25, 27, 29, 37, 43, 45, 49, 57, 73, 75, 77, 79, 81, 83, 87, 89, 91, 95, 101, 103, 107, 109, 111, 119, 121, 125, 129, 131, 135, 143, 145, 147, 151, 157, 161, 167, 169, 171, 179, 185, 187, 191, 199, 215, 217, 219, 221, 223, 225, 229, 231, 233, 237, 243, 245, 249, 251, 253, 261, 263, 267, 271, 273, 277.
$x^2 + 73 y^2$	$292 z +$ 1, 7, 9, 11, 15, 25, 31, 37, 39, 41, 43, 47, 49, 51, 57, 59, 61, 63, 65, 69, 77, 81, 83, 85, 87, 89, 95, 97, 99, 103, 105, 107, 109, 115, 121, 131, 135, 137, 139, 145, 149, 151, 159, 163, 165, 167, 169, 173, 175, 179, 181, 191, 199, 201, 213, 217, 221, 225, 237, 239, 247, 257, 259, 263, 265, 269, 271, 273, 275, 279, 287, 289.
$x^2 + 74 y^2$	$296 z +$ 1, 3, 5, 9, 11, 13, 15, 23, 25, 27, 29, 31, 33, 39, 41, 45, 49, 55, 61, 65, 67, 69, 73, 75, 79, 81, 83, 87, 89, 93, 99, 103, 107, 109, 115, 117, 119, 121, 123, 125, 133, 135, 137, 139, 143, 145, 147, 155, 165, 167, 169, 183, 191, 195, 199, 201, 205, 207, 211, 219, 225, 233, 237, 239, 243, 245, 249, 253, 261, 275, 277, 279, 289.
$x^2 + 77 y^2$	$308 z +$ 1, 3, 9, 13, 17, 25, 27, 31, 37, 39, 41, 43, 47, 51, 53, 59, 61, 73, 75, 79, 81, 93, 95, 101, 103, 107, 111, 113, 115, 117, 119, 123, 127, 129, 137, 141, 143, 145, 151, 153, 169, 173, 177, 183, 199, 211, 219, 221, 223, 225, 239, 241, 243, 251, 263, 279, 285, 289, 293, 297, 303.

$x^2 + 78y^2$	$312z +$ 1, 19, 25, 29, 35, 37, 41, 47, 49, 53, 55, 67, 71, 77, 79, 85, 89, 101, 103, 107, 109, 115, 119, 121, 127, 131, 137, 155, 161, 163, 167, 173, 179, 187, 199, 215, 217, 229, 239, 251, 253, 269, 281, 289, 295, 301, 305, 307.
$x^2 + 79y^2$	$316z +$ 1, 5, 9, 11, 13, 19, 21, 23, 25, 31, 45, 49, 51, 55, 65, 67, 73, 81, 83, 87, 89, 95, 97, 99, 101, 105, 111, 115, 117, 119, 121, 123, 125, 129, 131, 141, 143, 151, 155, 159, 163, 167, 169, 171, 173, 177, 179, 181, 183, 189, 203, 207, 209, 213, 223, 225, 231, 239, 241, 245, 247, 253, 255, 257, 259, 263, 269, 273, 275, 277, 297, 281, 283, 287, 289, 301, 309, 313.
$x^2 + 82y^2$	$328z +$ 1, 7, 9, 13, 15, 25, 29, 33, 43, 47, 49, 51, 53, 55, 57, 59, 63, 69, 71, 73, 79, 81, 83, 85, 91, 93, 95, 101, 105, 107, 109, 111, 113, 115, 117, 121, 131, 135, 139, 149, 151, 155, 157, 163, 167, 169, 175, 181, 183, 185, 187, 191, 195, 199, 201, 203, 209, 225, 229, 231, 239, 241, 251, 253, 261, 263, 267, 283, 289, 291, 293, 297, 301, 305, 307, 309, 311, 317, 323, 325.
$x^2 + 83y^2$	$332z +$ 1, 3, 7, 9, 11, 17, 21, 23, 25, 27, 29, 31, 33, 37, 41, 49, 51, 59, 61, 63, 65, 69, 75, 77, 81, 87, 93, 95, 99, 109, 111, 113, 119, 121, 123, 127, 131, 147, 151, 153, 161, 167, 169, 173, 175, 177, 183, 187, 189, 191, 193, 195, 197, 199, 203, 207, 215, 217, 225, 227, 229, 231, 235, 241, 243, 247, 253, 259, 261, 265, 275, 277, 279, 285, 287, 289, 293, 297, 313, 317, 319, 327.
$x^2 + 85y^2$	$340z +$ 1, 9, 11, 21, 31, 37, 39, 43, 47, 49, 57, 67, 69, 71, 73, 79, 81, 83, 87, 89, 91, 97, 99, 101, 103, 113, 121, 123, 127, 131, 133, 139, 149, 159, 161, 169, 173, 177, 183, 189, 193, 197, 199, 203, 211, 223, 229, 231, 233, 247, 263, 277, 279, 281, 287, 299, 307, 311, 313, 317, 321, 327, 333, 337.
$x^2 + 86y^2$	$344z +$ 1, 3, 5, 9, 15, 17, 19, 23, 25, 27, 29, 31, 37, 41, 45, 47, 49, 51, 57, 61, 69, 75, 77, 79, 81, 85, 89, 91, 93, 95, 97, 103, 111, 115, 121, 123, 125, 127, 131, 135, 141, 143, 145, 147, 149, 153, 155, 157, 163, 167, 169, 171, 179, 183, 185, 193, 205, 207, 211, 225, 227, 231, 235, 237, 239, 243, 245, 255, 261, 271, 273, 277, 279, 281, 285, 289, 291, 305, 309, 311, 323, 331, 333, 337.
$x^2 + 87y^2$	$348z +$ 1, 7, 11, 13, 17, 25, 41, 47, 49, 67, 77, 89, 91, 95, 101, 103, 109, 113, 115, 119, 121, 131, 137, 139, 143, 151, 155, 169, 175, 181, 185, 187, 191, 199, 215, 221, 223, 241, 251, 263, 265, 269, 275, 277, 283, 287, 289, 293, 295, 305, 311, 313, 317, 325, 329, 343.
$x^2 + 89y^2$	$363z +$ 1, 3, 5, 7, 9, 15, 17, 19, 21, 23, 25, 27, 31, 35, 43, 45, 49, 51, 53, 57, 59, 63, 69, 73, 75, 81, 83, 85, 93, 95, 97, 103, 105, 109, 115, 119, 121, 125, 127, 129, 133, 135, 143, 147, 151, 153, 155, 157, 159, 161, 163, 169, 171, 173, 175, 177, 189, 191, 207, 211, 215, 217, 219, 225, 233, 239, 243, 245, 249, 255, 257, 265, 269, 277, 279, 285, 289, 291, 295, 301, 309, 315, 317, 319, 323, 327, 343, 354.
$x^2 + 91y^2$	$364z +$ 1, 5, 7, 9, 19, 23, 25, 29, 31, 33, 41, 43, 45, 47, 51, 53, 59, 73, 79, 81, 83, 89, 95, 97, 107, 111, 113, 121, 125, 127, 145, 155, 165, 167, 171, 179, 183, 187, 139, 191, 201, 205, 207, 211, 213, 215, 223, 225, 227, 229, 233, 235, 241, 255, 261, 263, 265, 271, 277, 279, 289, 293, 295, 303, 307, 309, 327, 347, 349, 353, 361.

Form	Values
$x^2 + 93y^2$	$372z +$ 1, 17, 25, 29, 35, 43, 47, 49, 53, 55, 59, 65, 71, 77, 79, 89, 91, 95, 97, 107, 109 115, 121, 127, 131, 133, 137, 139, 143, 151, 157, 161, 169, 185, 191, 193, 197, 199, 205, 209, 223, 227, 247, 253, 259, 269, 271, 287, 289, 299, 305, 311, 331, 335, 349, 353, 359, 361, 365, 367.
$x^2 + 94y^2$	$376z +$ 1, 5, 7, 9, 11, 13, 17, 19, 25, 29, 35, 43, 45, 49, 55, 63, 65, 67, 69, 71, 77, 79, 81, 85, 89, 91, 93, 95, 97, 99, 103, 107, 109, 111, 117, 119, 121, 123, 125, 133, 139, 143, 145, 153, 159, 163, 169, 171, 175, 177, 179, 181, 183, 187, 191, 203, 209, 211, 215, 219, 221, 225, 227, 229, 239, 241, 245, 247, 249, 261, 263, 271, 275, 289, 293, 301, 303, 315, 317, 319, 323, 325, 335, 337, 339, 343, 345, 349, 353, 355, 361, 373.
$x^2 + 95y^2$	$380z +$ 1, 3, 9, 11, 13, 27, 33, 37, 39, 49, 53, 61, 67, 81, 97, 99, 101, 103, 107, 111, 113, 117, 119, 121, 127, 131, 139, 143, 147, 149, 159, 161, 167, 169, 173, 183, 191, 193, 199, 201, 203, 217, 223, 227, 229, 239, 243, 251, 257, 271, 287, 289, 291, 293, 297, 301, 303, 307, 309, 311, 317, 321, 329, 333, 337, 339, 349, 351, 357, 359, 363, 373.
$x^2 + 97y^2$	$388z +$ 1, 7, 9, 15, 19, 23, 25, 33, 39, 49, 51, 53, 55, 59, 61, 63, 65, 67, 71, 73, 81, 83, 85, 87, 89, 93, 101, 105, 107, 109, 111, 113, 121, 123, 127, 129, 131, 133, 135, 139, 141, 143, 145, 155, 161, 169, 171, 175, 179, 185, 187, 193, 197, 199, 205, 207, 211, 215, 221, 223, 225, 229, 231, 235, 237, 239, 241, 251, 263, 269, 271, 273, 285, 289, 293, 297, 309, 311, 313, 319, 331, 341, 343, 345, 347, 351, 353, 357, 359, 361, 367, 371, 375, 377, 383, 385.
$x^2 + 101y^2$	$404z +$ 1, 3, 5, 7, 9, 11, 13, 15 17, 21, 25, 27, 33, 35, 37, 39, 45, 49, 51, 55, 59, 63, 65, 67, 75, 77, 81, 83, 85, 91, 97, 99, 103, 105, 111, 117, 119, 121, 125, 127, 135, 137, 139, 143, 147, 151, 153, 157, 163, 165, 167, 169, 175, 177, 181, 185, 187, 189, 191, 193, 195, 197, 199, 201, 221, 225, 231, 233, 243, 245, 249, 255, 259, 263, 271, 273, 275, 287, 289, 291, 295, 297, 305, 311, 313, 315, 321, 329, 331, 335, 343, 347, 351, 357, 361, 363, 373, 375, 381, 385

Lineare Theiler

der quadratischen Form $x^2 - ay^2$ für alle Werthe von a von 1 bis 101.

Form	Theiler
$x^2 - 2y^2$	$8z +$ 1, 7.
$x^2 - 3y^2$	$12z +$ 1, 11.
$x^2 - 5y^2$	$20z +$ 1, 9, 11, 19.
$x^2 - 6y^2$	$24z +$ 1, 5, 19, 23.
$x^2 - 7y^2$	$28z +$ 1, 3, 9, 19, 25, 27.
$x^2 - 10y^2$	$40z +$ 1, 3, 9, 13, 27, 31, 37, 39.
$x^2 - 11y^2$	$44z +$ 1, 5, 7, 9, 19, 25, 35, 37, 39, 43.
$x^2 - 13y^2$	$52z +$ 1, 3, 9, 17, 23, 25, 27, 29, 35, 43, 49, 51.
$x^2 - 14y^2$	$56z +$ 1, 5, 9, 11, 13, 25, 31, 43, 45, 47, 51, 55.
$x^2 - 15y^2$	$60z +$ 1, 7, 11, 17, 43, 49, 53, 59.
$x^2 - 17y^2$	$68z +$ 1, 9, 13, 15, 19, 21, 25, 33, 35, 43, 47, 49, 53, 55, 59, 67.
$x^2 - 19y^2$	$76z +$ 1, 3, 5, 9, 15, 17, 25, 27, 31, 45, 49, 51, 59, 61, 67, 71, 73, 75.
$x^2 - 21y^2$	$84z +$ 1, 5, 17, 25, 37, 41, 43, 47, 59, 67, 79, 83.
$x^2 - 22y^2$	$88z +$ 1, 3, 7, 9, 13, 21, 25, 27, 29, 39, 49, 59, 61, 63, 67, 75, 79, 81, 85, 87.
$x^2 - 23y^2$	$92z +$ 1, 7, 9, 11, 13, 15, 19, 25, 29, 41, 43, 49, 51, 63, 67, 73, 77, 79, 81, 83, 85, 91.
$x^2 - 26y^2$	$104z +$ 1, 5, 9, 11, 17, 19, 21, 23, 25, 37, 45, 49, 55, 59, 67, 79, 81, 83, 85, 87, 93, 95, 99, 103.
$x^2 - 29y^2$	$116z +$ 1, 5, 7, 9, 13, 23, 25, 33, 35, 45, 49, 51, 53, 57, 59, 63, 65, 67, 71, 81, 83, 91, 93, 103, 107, 109, 111, 115.
$x^2 - 30y^2$	$120z +$ 1, 7, 13, 17, 19, 29, 37, 49, 71, 83, 91, 101, 103, 107, 113, 119.
$x^2 - 31y^2$	$124z +$ 1, 3, 5, 9, 11, 15, 23, 25, 27, 33, 41, 43, 45, 49, 55, 69, 75, 79, 81, 83, 91, 97, 99, 101, 109, 113, 115, 119, 121, 123.
$x^2 - 33y^2$	$132z +$ 1, 17, 25, 29, 31, 35, 37, 41, 49, 65, 67, 83, 91, 95, 97, 101, 103, 107, 115, 131.
$x^2 - 34y^2$	$136z +$ 1, 3, 5, 9, 11, 15, 25, 27, 29, 33, 37, 45, 47, 49, 55, 61, 75, 81, 87, 89, 91, 99, 103, 107, 109, 111, 121, 125, 127, 131, 133, 135.
$x^2 - 35y^2$	$140z +$ 1, 9, 13, 17, 19, 23, 29, 31, 33, 43, 59, 67, 73, 81, 97, 107, 109, 111, 117, 121, 123, 127, 131, 139.

Bemerkung

zur Terminologie.

Wiewohl der Herausgeber in diesem Buche sich geflissentlich der üblichen Terminologie bediente, wünscht er doch nicht es in die Oeffentlichkeit treten zu lassen, ohne folgenden Vorschlag auszusprechen:

Sollte es sich nicht empfehlen, Zahlen, „welche einen gemeinsamen Theiler besitzen", kurz **gemeintheilig** und in Uebereinstimmung hiermit die „relativen Primzahlen", oder gar „relativ-primen Zahlen" **nichtgemeintheilig** zu nennen?

Auch ist es vielleicht zweckmässig **Gemeintheiler** anstatt „gemeinsamer Theiler" einzuführen.

Entsprechend könnte man Ausdrücke beim *Vielfachen* bilden.

Internationale Wortformen wären *condivisibel* u. s. w.

Göttingen, Druck der Univ.-Buchdruckerei von E. A. Huth.